OPERATION ODYSSEY DAWN OPERATION GLADIATOR SHIELD OPERATION TOMODACHI OPERATION UNIFIED PROTECT

THE JOINT ENTERPRISE: DELIVERED THROUGH PARTNERSHIP

PROGRAM GUIDE

May 7-10, 2012
TAMPA CONVENTION CENTER
TAMPA, FLORIDA

2012 DISA MISSION PARTNER CONFERENCE

DISA

OPERATION NEW DAWN OPERATION UNIFIED RESPONSE OPERATION ENDURING FREEDOM

WELCOME

Welcome to the 2012 DISA Mission Partner Conference.

Everyone in DISA realizes that delivering an enterprise that improves security, enhances effectiveness, achieves efficiency, enables innovation, and reduces the warfighter's burden can be achieved by working with our mission partners.

Delivering this enterprise infrastructure and providing enterprise services is our highest priority, and we recognize that creating, enhancing, and sustaining the joint enterprise requires a "team effort." All DoD mission partners must work together to develop joint solutions and shared approaches. It also requires us to collaborate with industry partners to develop, operate, and sustain the services and capabilities we provide/use; as well as to coordinate with other government and non-governmental stakeholders, users, suppliers, and experts.

That's why the conference theme is
"The Joint Enterprise: Delivered Through Partnership."

WELCOME

Over the past year, DISA and its partners have taken significant steps to realize a truly joint enterprise information environment. Now we must step it up a level and continue to move forward in order to achieve an environment where the user can connect with any device, anytime, anywhere on the globe and be productive. This environment will be characterized by:

- Improved security, achieved by a single, well-defended, agile enterprise infrastructure that responds quickly to change.
- Improved efficiencies by eliminating duplication of capabilities.
- Increased mission effectiveness as a result of standard, ubiquitous solutions.
- Centralized IT that enhances mission focus and leaves the heavy lifting to the enterprise.
- Agile IT because technology is centrally implemented and rapidly exploited.

This conference is a great opportunity for all of us to be informed and challenged by the presentations of Defense and Industry leaders, to share our thoughts and ideas in the track sessions, to exchange our perspectives with one another, and to discuss services and emerging technologies with vendor representatives in the exhibit hall.

Together we'll deliver the joint enterprise!

Ronnie D. Hawkins, Jr.
Lieutenant General, USAF
Director, DISA

USEFUL INFORMATION

IN THIS BOOK

REGISTRATION HOURS

Sunday, May 6	3 p.m. – 5 p.m.	2nd Floor
Monday, May 7	8 a.m. – 7:30 p.m.	2nd Floor
Tuesday, May 8	6:30 a.m. – 5 p.m.	2nd Floor
Wednesday, May 9	6:30 a.m. – 5 p.m.	2nd Floor
Thursday, May 10	6:30 a.m. – 1 p.m.	2nd Floor

EXHIBIT HOURS

Monday, May 7	5:30 p.m. – 7:30 p.m.	Exhibit Hall, 3rd Floor
Tuesday, May 8	9:30 a.m. – 5 p.m.	Exhibit Hall, 3rd Floor
Wednesday, May 9	8:30 a.m. – 4 p.m.	Exhibit Hall, 3rd Floor
Thursday, May 10	9:30 a.m. – 1 p.m.	Exhibit Hall, 3rd Floor

USEFUL INFORMATION

Location Information
Tampa Convention Center
333 South Franklin Street
Tampa, Florida 33602
Phone: (813) 274-8511

Attire
The uniform for military personnel attending the DISA Mission Partner Conference is uniform of the day. Civilian attire for the conference is business casual.

DISA Conference Operations Support Center
The conference operations support center (Ops Center) is located in room 1. Limited office supplies, copier, printer, and telephone are available for use by conference attendees.

Business Hours:

Sunday, May 6	12 p.m. – 4 p.m.
Monday, May 7	7 a.m. – 6 p.m.
Tuesday, May 8	6 a.m. – 6 p.m.
Wednesday, May 9	6 a.m. – 6 p.m.
Thursday, May 10	6 a.m. – 2 p.m.

AFCEA Technology Showcase **Cyber Cafe** Sponsored by ManTech International Corporation

Access to personal email is available in the Cyber Café. The Cyber Café is located in the exhibit hall during exhibit hall hours.

*Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.

- Have lunch with Tony Montemarano and the DISA Senior Leaders on **Monday, May 7** from **12–1:30 p.m.** in the first floor ballroom.
- During the plenary sessions and lunch on Tuesday and Thursday, DISA Senior Leaders welcome you to sit at their tables. A diagram of the tables with the leaders' locations can be found outside the main entry doors to the plenary session area.
- DISA Senior Leaders will engage with industry in the AFCEA Technology Showcase on **Monday, May 7** from **5:30–7:30 p.m.** and **Tuesday, May 8** from **1:30–5 p.m.**

CONNECTION CENTRAL

Meet with and ask DISA Senior Leaders questions on what's new in DISA Connection Central, located in the DISA Pavilion of the Exhibit Hall on ***Tuesday, May 8.***

11:30 a.m. – 12 p.m.

Dr. Jennifer Carter, Component Acquisition Executive
Mark Orndorff, Chief Information Assurance Executive/
Director PEO Mission Assurance and Network Operations
Alfred Rivera, Director, Enterprise Services

1:30 p.m. – 2 p.m.

Cindy Moran, Director, Network Services
Gerald Doyle, Director, Enterprise Engineering

2 p.m. – 2:30 p.m.

Jimaye Sones, Chief Financial Executive/Comptroller
Kathleen Miller, Director, Procurement and Chief, DITCO

2:30 p.m. – 3 p.m.

Bruce Bennett, PEO, Satellite Communications, Teleport and Services
Henry Sienkiewicz, Chief Information Officer
Luanne Overstreet, Test and Evaluation Executive

3 p.m. – 3:30 p.m.

Larry Huffman, Principal Director, Operations
Martin Gross, PEO, Command and Control Capabilities
Jack Wilmer, PEO, GIG Enterprise Services

3:30 p.m. – 4 p.m.

Tony Montemarano, Director, Strategic Planning and Information
Dave Mihelcic, Chief Technology Officer
Alan Lewis, PEO, GIG Enterprise Services

4:30 p.m. – 5 p.m.

Col David Stickley, Director, Cross Functional Solutions
Dr. Glen White, Command and Control Capabilities
Sherrie Balko, Vice Director, PEO Mission Assurance/NetOps

AGENDA

MONDAY May 7

8 a.m.. – 7:30 p.m.	Conference Registration	2nd Floor
AFCEA Technology Showcase	**Conference Registration** Sponsored by BROCADE	
12 p.m.. – 1:30 p.m.	Lunch with DISA Senior Leaders	Ballroom, 1st Floor
2:30 p.m – 4:30 p.m	Tracks and Sessions	Meeting Rooms, 1st Floor
5:30 pm. – 7:30 p.m.	Grand Opening: AFCEA Technology Showcase	Exhibit Hall, 3rd Floor
AFCEA Technology Showcase	Grand Opening Reception Station Sponsor AAC Network Focused. Solution Driven.	

*Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.

TUESDAY May 8

6:30 a.m. – 5 p.m.	Conference Registration	2nd Floor
AFCEA Technology Showcase	**Conference Registration** Sponsored by BROCADE	
9:30 a.m. – 5 p.m.	AFCEA Technology Showcase	Exhibit Hall, 3rd Floor
6:30 a.m. – 7:45 a.m.	Continental Breakfast	Ballroom Foyer, 1st Floor
AFCEA Technology Showcase	**Continental Breakfast** Sponsored by neustar	
8 a.m. – 9 a.m.	Opening Ceremony, Keynote Address **Lt Gen Ronnie D. Hawkins, Jr., USAF** Director Defense Information Systems Agency	East Hall, 3rd Floor
9 a.m. – 9:45 a.m.	**Dr. Edward Amoroso** Chief Security Officer AT&T Inc.	East Hall, 3rd Floor
9:45 a.m. – 10:15 a.m.	Coffee Break in Exhibit Hall	Exhibit Hall, 3rd Floor
10:15 a.m. – 11 a.m.	**Dr. Tom Leighton** Co-Founder & Chief Scientist Akamai	East Hall, 3rd Floor
11 a.m – 12 p.m.	Networking Break in Exhibit Hall	Exhibit Hall, 3rd Floor
12 p.m. – 1:30 p.m.	Lunch **Dr. Pradeep Sindu, Ph.D.** Vice Chairman, Chief Technology Officer, and Founder Juniper Networks	East Hall, 3rd Floor
AFCEA Technology Showcase	**Lunch** Sponsored by QinetiQ North America	
1:30 p.m. – 3 p.m.	Tracks and Sessions	Meeting Rooms, 1st Floor
3 p.m. – 3:30 p.m.	Refreshment Break	Exhibit Hall & 1st Floor Hallways
3:30 p.m. – 5 p.m.	Tracks and Sessions	Meeting Rooms, 1st Floor

*Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.

AGENDA

WEDNESDAY May 9

6:30 a.m. – 5 p.m.	Conference Registration	2nd Floor
AFCEA Technology Showcase	**Conference Registration** Sponsored by BROCADE	
8:30 a.m. – 4 p.m.	AFCEA Technology Showcase	Exhibit Hall, 3rd Floor
6:30 a.m. – 7:45 a.m.	Continental Breakfast	Ballroom Foyer, 1st Floor
AFCEA Technology Showcase	**Continental Breakfast** Sponsored by HARRIS CAPROCK	
7:45 a.m. – 8 a.m.	Opening Remarks	East Hall, 3rd Floor
8 a.m. – 8:45 a.m.	**Mark Hurd** President Oracle Corporation	East Hall, 3rd Floor
8:45 a.m. – 9:15 a.m.	Coffee Break	Exhibit Hall, 3rd Floor
AFCEA Technology Showcase	**Coffee Break** Sponsored by HARRIS CAPROCK	
9:15 a.m. – 10:45 a.m.	DoD CIO Panel **Teri Takai** Chief Information Officer Department of Defense **LTG Susan S. Lawrence, USA** Chief Information Officer/G-6 U.S. Army **Lt Gen Michael J. Basla, USAF** Vice Commander Air Force Space Command **Terry Halvorsen** Chief Information Officer Department of the Navy **BGen Kevin J. Nally, USMC** Director, C4/Chief Information Officer U.S. Marine Corps **RDML Diane E. H. Webber, USN** Director, Communications and Networks Division (OPNAV N2/N6F1) U.S. Navy	East Hall, 3rd Floor
10:45 a.m. – 11:30 p.m	**Lowell C. McAdam** Chairman and Chief Executive Officer Verizon	East Hall, 3rd Floor
11:30 p.m – 1 p.m.	Lunch	Exhibit Hall, 3rd Floor
AFCEA Technology Showcase	**Lunch** Sponsored by HARRIS CAPROCK	

**Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.*

WEDNESDAY May 9

1 p.m. – 2 p.m.	Tracks and Sessions	Meeting Rooms, 1st Floor
2 p.m. – 2:30 p.m.	Break	
2:30 p.m. – 3:30 p.m.	Tracks and Sessions	Meeting Rooms, 1st Floor
3:30 p.m. – 4 p.m.	Refreshment Break	Exhibit Hall & 1st Floor Hallways
AFCEA **Technology Showcase**	**Beverage Break** Sponsored by HARRIS CAPROCK	
4 p.m. – 5 p.m.	Tracks and Sessions	Meeting Rooms, 1st Floor
6:30 p.m. - 8:30 p.m.	AFCEA **Technology Showcase** Networking Event	Ballroom, 1st Floor

Forecast to Industry (East Hall, 3rd Floor)

1 p.m. – 1:03 p.m.	Introduction *(Lt Gen Ronnie D. Hawkins, Jr., DISA Director)*
1:03 p.m. – 1:18 p.m.	Welcome *(Kathleen Miller, Director, Procurement and DITCO)*
1:18 p.m. – 1:25 p.m.	Remarks *(Dr. Jennifer Carter, Component Acquisition Executive)*
1:25 p.m. – 1:40 p.m.	DISA's Technology & Current Vision *(Dave Mihelcic, Chief Technology Officer)*
1:40 p.m. – 2 p.m.	Mission Assurance *(Mark Orndorff, Chief IA Executive and PEO, MA)*
2 p.m. – 2:15 p.m.	Command & Control Capabilities *(Martin Gross, Program Executive Officer, C2C)*
2:15 p.m. – 2:30 p.m.	Defense Spectrum Organization *(Stuart Timerman, Director, DSO)*
2:30 p.m. – 2:45 p.m.	Operations *(Larry Huffman, Director, Operations)*
2:45 p.m. – 3 p.m.	Enterprise Services *(Alfred Rivera, Director, ES)*
3 p.m. – 3:20 p.m	Network Services *(Cindy Moran, Director, NS)*
3:20 p.m – 3:35 p.m.	Communications *(Bruce Bennett, Program Executive Officer, COMMs)*
3:35 p.m. – 3:50 p.m.	Chief Information Office *(Henry Sienkiewicz, Chief Information Officer)*
3:50 p.m. – 4:05 p.m.	Office of Small Business Programs *(Sharon Jones, Chief, OSBP)*
4:05 p.m. – 4:15 p.m.	Wrap Up

**Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.*

AGENDA

THURSDAY May 10

6:30 a.m. – 1 p.m.	Conference Registration	2nd Floor
AFCEA Technology Showcase	**Conference Registration** Sponsored by BROCADE	
9:30 a.m. – 1 p.m.	AFCEA Technology Showcase	Exhibit Hall, 3rd Floor
6:30 a.m. – 7:45 a.m.	Continental Breakfast	Ballroom Foyer, 1st Floor
8 a.m. – 8:30 a.m.	**Opening Remarks**	East Hall, 3rd Floor
8:30 a.m. – 10 a.m.	IT Efficiencies Exchange Panel **MG Mark S. Bowman, USA** Director, C4, Chief Information Officer The Joint Staff **Mike Krieger** Deputy Chief Information Officer/G-6 U.S. Army **Janice C. Haith** Director, Deputy Chief Information Officer Division Department of the Navy **Cora Carmody** Senior Vice President, Information Technology Jacobs Engineering **Jeff Barr** Senior Web Services Evangelist Amazon Web Services	East Hall, 3rd Floor
10 a.m. – 11 a.m.	Coffee Break in Exhibit Hall	Exhibit Hall, 3rd Floor
11 p.m. – 12:30 p.m.	Lunch **GEN Keith B. Alexander, USA** Commander U.S. Cyber Command	East Hall, 3rd Floor
AFCEA Technology Showcase	**Lunch** Sponsored by LOCKHEED MARTIN	
12:30 p.m. – 1 p.m.	Closing Remarks	East Hall, 3rd Floor

**Sponsor logos are part of the AFCEA Technology Showcase. DISA and the Department of Defense in no way endorse AFCEA, its events, programs, or sponsors.*

TUESDAY

Lt Gen Ronnie D. Hawkins, Jr., USAF
Director
Defense Information Systems Agency

Lt Gen Ronnie D. Hawkins Jr. is director, Defense Information Systems Agency, Fort Meade, Md. He leads a global organization of military and civilian personnel who plan, develop, deliver, and operate joint interoperable command and control capabilities and a global enterprise infrastructure in direct support of the President, Secretary of Defense, Joint Chiefs of Staff, Combatant Commanders, Department of Defense components, and other mission partners across the full spectrum of operations.

Dr. Edward G. Amoroso
Chief Security Officer
AT&T Inc.

Dr. Edward G. Amoroso serves as senior vice president and chief security officer for AT&T Services, Inc. His responsibilities include real-time security protection of AT&T's network and computing infrastructure – including mobility services; security policy, planning, and architecture for AT&T's enterprise; security support for AT&T's IPTV initiatives; and lead design, development, and operations support for AT&T's managed and network-based security services.

Dr. Tom Leighton
Co-Founder and Chief Scientist
Akamai

Dr. Tom Leighton co-founded Akamai Technologies in August 1998. Serving as chief scientist and as a member of the Board of Directors, Dr. Leighton is Akamai's technology visionary and works with the senior management team to set the company's direction. Dr. Leighton is a Professor of Applied Mathematics at MIT and has been a member of the Computer Science and Artificial Intelligence Laboratory (CSAIL) since its inception in 1996.

Dr. Pradeep Sindhu
Vice Chairman, Chief Technology Officer, and Founder
Juniper Networks

Dr. Pradeep Sindhu founded Juniper Networks in February 1996 and has held several central roles in shaping the company. He currently serves as vice chairman of the board and chief technology officer, and is responsible for the company's technical roadmap as well as day-to-day design and development of future products. Upon founding the company, he served as chairman and chief executive officer. During that time, he played a central role in the architecture, design, and development of the M40 router. Before founding Juniper Networks, Sindhu was a principal scientist and distinguished engineer at the Computer Science Lab at Xerox's Palo Alto Research Center (PARC).

BIOGRAPHIES

WEDNESDAY

Teri Takai
Chief Information Officer
Department of Defense

Ms. Teri Takai serves as the principal advisor to the Secretary of Defense for Information Management/ Information Technology and Information Assurance as well as non-intelligence Space systems, critical satellite communications, navigation, and timing programs, spectrum, and telecommunications. She provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology-based capabilities required to support the broad set of Department missions. Ms. Takai previously served as chief information officer for the State of California.

LTG Susan S. Lawrence, USA
Chief Information Officer/G-6
U.S. Army

As the CIO, LTG Lawrence reports directly to the Secretary of the Army for setting strategic direction and objectives, and supervises all Army C4 (command, control, communications, and computers) and IT functions. As the G-6, she supports the Chief of Staff of the Army by advising on network, communications, and signal operations. This includes advising on the impact of communications security, force structure, equipping, and employment of network, communications, and signal capabilities on Army operations.

Lt Gen Michael J. Basla, USAF
Vice Commander
Air Force Space Command

Lt Gen Michael J. Basla was recently selected as chief, Information Dominance and chief information officer, Office of the Secretary of the Air Force. He currently serves as the vice commander of the Air Force Space Command, Peterson Air Force Base, Colo. He assists the commander in organizing, equipping, training, and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command, and the other functional and geographic combatant commands with missile warning, positioning, navigation and timing, communications, and cyber capabilities. The command oversees Air Force network operations; manages a global network of satellite command and control, communications, missile warning and space launch facilities; and is responsible for space system development and acquisition.

Terry Halvorsen
Chief Information Officer
Department of the Navy

As the Department of the Navy (DON) chief information officer (CIO), Halvorsen heads the Office of the DON CIO and is the DON's senior official and advisor on matters related to information management (IM), information technology (IT)/cyberspace (including national security systems) and information resources management (IRM). Halvorsen has oversight for the IM function within the Office of the Secretary of the Navy, Chief of Naval Operations, and Headquarters Marine Corps. He develops strategies, policies, plans, architectures, standards, and guidance, and provides process transformation support for the entire Department of the Navy. Additionally, he ensures that the development and acquisition of IT systems are interoperable and consistent with the Department's objectives and vision.

BGen Kevin J. Nally, USMC
Director, C4/Chief Information Officer
U.S. Marine Corps

BGen Kevin Nally is the director for Command, Control, Communications, and Computers (C4) for the United States Marine Corps. BGen Nally was commissioned a second lieutenant in the Marine Corps in May 1981, after graduating from Eastern Kentucky University with a Bachelor of Science in Agronomy and Natural Resources. After completing The Basic School and Communications Officer Course, he was assigned to the 1st Marine Amphibious Brigade where he served as a Communications Platoon Commander for the Marine Service Support Group-37 and later as a Communications Platoon Commander for the Brigade Service Support Group.

WEDNESDAY

RDML Diane E. H. Webber, USN

Director, Communications and Networks Division (OPNAV N2/N6F1)
U.S. Navy

RMDL Diane Webber reported to the Office of the Chief of Naval Operations and was assigned as division director for Communications and Networks (OPNAV N2/N6F1). Webber's operational tours include early assignments as an oceanographic watch officer at U.S. Naval Facility, Argentia, Newfoundland and commander, Oceanographic Systems, Pacific. During Operation Iraqi Freedom, she commanded U.S. Naval Computer and Telecommunications Station, Bahrain. Webber was assigned to MultiNational Forces, Iraq as director, Communications and Information Systems (CIS) Coalition Force Plans/Joint Network Control Center (JNCC) and subsequently served as director, Communications Information Systems, 2nd Fleet.

Mark Hurd

President
Oracle Corporation

Mark Hurd is president of Oracle Corporation and a member of the company's Board of Directors. He joined Oracle in 2010, bringing more than 30 years of technology industry leadership, computer hardware expertise, and executive management experience to his role with the company. As president, Hurd oversees the corporate direction and strategy for Oracle's global field operations, including marketing, sales, consulting, alliances and channels, and support. He focuses on strategy, leadership, innovation, and customers. Before joining Oracle, Hurd served as chairman of the Board, chief executive officer, and president of HP, where his focus on customers, innovation, improved operational efficiency, and execution led to significant company growth.

Lowell C. McAdam

Chairman and Chief Executive Officer
Verizon

Lowell C. McAdam is chairman and chief executive officer of Verizon Communications with responsibility for the operations of Verizon, including all business units and staff functions. In addition, he is chairman of the Verizon Wireless Board of Representatives.From October 2010 until he assumed his current position, McAdam served as president and chief operating officer and had responsibility for the operations of the company's network-based businesses — Verizon Wireless and Verizon Telecom and Business — as well as Verizon Services Operations. He was also responsible for the technology management and chief information officer functions.

THURSDAY

GEN Keith B. Alexander, USA

Commander, U.S. Cyber Command (USCYBERCOM)
Director, National Security Agency/Chief, Central Security Service (NSA/CSS)

As commander, USCYBERCOM, GEN Alexander is responsible for planning, coordinating, and conducting operations and defense of DoD computer networks as directed by U.S. Strategic Command (USSTRATCOM). As the director of NSA and chief of CSS, he is responsible for a DoD agency with national foreign intelligence, combat support, and U.S. national security information system protection responsibilities. NSA/CSS civilian and military personnel are stationed worldwide.

THURSDAY (continued)

MG Mark S. Bowman, USA
Director, Command, Control, Communications, and Computers (C4)
and Chief Information Officer (CIO)
The Joint Staff

MG Mark S. Bowman is the director Command, Control, Communications and Computers (C4), chief information officer, Joint Staff, J6/CIO. He develops C4 capabilities; conducts analysis and assessments; provides joint and combined force C4 guidance; and evaluates C4 requirements, plans, programs, and strategies for the Chairman of the Joint Chiefs of Staff. Most recently, he served as the director of Architecture, Operations, Networks, and Space, Office of the Army CIO/G-6 for establishing and maintaining strategy, policy, and guidance to build, integrate, communicate, and facilitate the seamless implementation of the Army's network (LandWarNet) in a joint and coalition environment

Mike Krieger
Deputy Chief Information Officer/G-6
U.S. Army

Mike Krieger became the Army deputy chief information officer/G-6 in July 2008. He also served as the acting Army CIO/G-6 from November 2010 through March 2011. He oversees the implementation of the Army's strategic direction for the network and the enterprise network infrastructure. The Army CIO/G-6 oversees the Army's $10 billion IT investments, manages the enterprise IT architecture, establishes and enforces IT policies, and directs the delivery of operational C4IT capabilities to support warfighters and enable joint information dominance. Krieger has broad experience in IT; he served 25 years in the U.S. Army, with operational assignments in tactical communications and command and control.

Janice C. Haith
Director, Deputy Chief Information Officer Division
Department of the Navy

Janice Haith is responsible for all chief information officer matters related to Navy. This includes governance, enterprise architecture, information assurance, information management/information technology, and Clinger-Cohen Act compliance. A security, intelligence, and CIO professional since 1984, Haith has completed assignments of increasing complexity in an extensive range of organizations. This included tenure as a security adjudicator for the Department of Justice; a program element manager (Security and Investigations) for Department of the Air Force; program manager for USAF (Joint Personnel Adjudication System) and DoD simultaneously; DoD e-Government program manager for Internal Efficiency and Effectiveness, and tenure as a congressional fellow on behalf of USAF.

Cora Carmody
Senior Vice President, Information Technology
Jacobs Engineering

As the senior vice president, Information Technology for Jacobs Engineering, Cora Carmody provides leadership for Jacobs' mission-critical IT systems including enterprise resources systems such as human resources; financial; operational support systems such as project control, engineering/design and collaboration; infrastructure systems; and services such as networks, servers, desktops, and web/social and collaborative systems. Carmody was with Litton/PRC from 1978 to 2001 and chief information officer there from 1996 to 2001, Invensys plc from 2001 to 2003 and SAIC from 2003 to 2008.

Jeff Barr
Senior Web Services Evangelist
Amazon Web Services

Jeff Barr is the senior web services evangelist at Amazon Web Services, where he is focused on furthering awareness among software developers of the opportunity to innovate and build businesses using Amazon Web Services. In this role, Barr travels, speaks, blogs, and conducts virtual events. He has a longstanding interest in web services and programmatic information interchange. He has held development and management positions at Microsoft, KnowNow, eByz, and Akopia and was a co-founder of Visix Software. Barr has been a technical reviewer for four books on web services, wrote a chapter on advanced scripting for a book on Second Life, and is the author of Host Your Website in the Cloud, published by SitePoint in September of 2010.

About the Tracks & Sessions

For years now, we've reiterated that our tracks and sessions are the heart of our conference. This year is no exception. We've really concentrated the content for our tracks this year to better facilitate discussions and hone in on those vital areas necessary to dialogue about, those important challenges we face as a combat support agency. Again, this year, our tracks are aligned and based on the DISA Campaign Plan Lines of Operation. The Campaign Plan is a living document that functions as our comprehensive, integrated strategic plan that will guide us in accomplishing the agency's mission and vision. Our three lines of operation — Enterprise Infrastructure, Command and Control and Information Sharing, and Operate and Assure — serve as the overarching foundation for realizing our goals. They are the framework in which the tracks are organized. Additionally, we have tracks that touch on our Joint Enablers — elements that support the Lines of Operation. As always, our tracks sessions are content-rich, collaborative learning experiences. New this year are industry tracks presented by various company leaders, presentations that will further aid in the dialogue to get to the solutions that will ultimately benefit the warfighter.

SATCOM Updates with Panel
After a brief overview on where DISA is heading with satellite communication (SATCOM) in the near future from each subject matter expert panel member, the panel will open the floor to all attendees to ask questions. A 10-minute break will be placed into the track session agenda.

IP Technical Evolution Project Implementations and Optical Transport Evolution
This session will cover an overview of current Internet Protocol (NIPR/SIPR/DISA Test and Evaulation Network (DTEN)) and Transport (DISN Core/Optical Transport Network (OTN)/Defense Information Systems Network Asynchronous Transfer Mode Service (DATMS) Elimination) sustainment efforts and future capabilities (Multi-Protocol Label Switching (MPLS)/Virtual Private Network (VPN)/Internet Protocol version 6). This talk addresses evolution of the optical transport technology from current 10G to future 1Tb/wavelength. First, the current 10G transport technology in the DISN core will be briefly discussed. Next, the drivers for upgrade to the next generation 100G optical transmission will be introduced and various available alternatives will be presented. Finally, emerging trends in 400G/1Tb transmission will be discussed.

Enterprise Classified/Unclassified Voice and IP Video Pilot
Enterprise Voice can provide a full range of voice-related capabilities to more than four million DoD users from central locations that fully leverage the Defense Information Systems Network (DISN) and IP technologies. This approach avoids the duplication of costs for voice services, operations and maintenance, network operations, sustainment, and information assurance at nearly 2,000 locations worldwide with a lower total cost of ownership. The purpose of this briefing is to present an update of ongoing initiatives to implement Enterprise Classified/ Unclassified Voice services.

This session will also highlight how DISA will transition DISN Video Services Global (DVS-G) to an Internet Protocol-based solution. It will highlight ongoing pilot activities that will meet DISA's priorities for migrating unclassified and classified Integrated Services Digital Network (ISDN) video teleconference users. Additionally, it will provide an update on multi-vendor testing events focused on ensuring video products comply with Assured Services Session Initiation Protocol (AS-SIP) standards in accordance with the Unified Capabilities Requirements (UCR) documents.

DVB-RCS and IW Updates
Briefings will be provided by program subject matter experts for Digital Video Broadcast - Return Channel Satellite System (DVB-RCS) and Integrated Waveform.

Network Services Customer Service Update and DISN Subscription Service Overview
This session will provide an overview of Network Services (NS) Customer Relationship Management (CRM) activities and approach; update Service Level Management (SLM) and Service Catalog Management (SCM) products; and customer projects. This session will also include a 20-minute discussion of the costs that comprise the subscription rate, how we determine site composition, the review process, and this year's differences based on DISA comptroller changes.

Commercial SATCOM Center Update
This update is a one-hour hour session to include a briefing and quesion-and-answer session. The briefing will provide a DISA satellite communication (SATCOM) Center and Future Commercial Satellite Communications (COMSATCOM) Services Acquisition (FCSA) overview that focuses on the four General Services Administration's contract vehicles under the FCSA strategy (SIN 132-54, SIN 132-55, Custom SATCOM Solutions (CS2) Indefinite Delivery/Indefinite Quantity (ID/IQ) Full and Open, and CS2-Small Business (SB)). In addition, a review of Enhanced Mobile Satellite Services (EMSS) products and services will be provided with a focus on the Distributed Tactical Communications System (DTCS).

Communications Track Schedule

Monday

2:30 p.m. – 4 p.m.	SATCOM Updates with Panel	Room 24/25

Tuesday

1:45 p.m. – 3:15 p.m.	IP Technical Evolution Project Implementations and Optical Transport Evolution	Room 24/25
3:30 p.m. – 5 p.m.	Enterprise Classified/Unclassified Voice and IP Video Pilot	Room 24/25

Wednesday

1 p.m. – 2 p.m.	DVB-RCS and IW Updates	Room 24/25
2:30 p.m. – 3:30 p.m.	Network Services Customer Service Update and DISN Subscription Service Overview	Room 24/25
4 p.m. – 5 p.m.	Commercial SATCOM Center Update	Room 24/25

Enterprise Services Overview
In this session, the Enterprise Services Directorate director will discuss the value of the convergence of Computing Services and the Program Executive Office - GIG Enterprise Services (PEO-GES) as well as the new strategic vision and focus. Discussions will include the latest news on cloud computing, virtualization, Identity and Access Management (IdAM), and Platform as a Service (PaaS). Also included is the ESD vision for collaboration and interoperability across the DoD enterprise.

IT Efficiencies
The Department's intention is to provide a single, secure, reliable, timely, effective, and agile command, control, communications, and computing (C4) enterprise information environment for use by the joint forces and non-DoD mission partners across the full spectrum of operations, at all echelons, and in all operational environments. The name of this environment is the Joint Information Enterprise. This briefing will provide an overview of the DoD's effort and highlight DISA's role as a key participant.

DoD Enterprise Email (DEE)
DoD Enterprise Email is a globally accessible managed service offering that provides both desktop based Outlook email and Outlook Web Access (OWA) email. The system uses capabilities from the Identity Access Manager (IdAM) offering from DISA; the Enterprise User account data provided by the Identity Synchronization Service (IdSS); and the Enterprise Application and Services Forest (EASF). The U.S. Army is currently migrating all of its members to this service, as well as the Joint Staff.

DoD Enterprise Portal Service (DEPS)
DoD Enterprise Portal Service (DEPS) provides a new NIPRNet implementation of Microsoft SharePoint 2010 offered by DISA Enterprise Services Directorate (DISA ESD) and deployed at DISA Enterprise Service Centers (ESCs) at ESC Mechanicsburg, Pa. and ESC Oklahoma City, Okla. The service provides a multi-tenant SharePoint environment offering both enterprise and standard versions of SharePoint 2010. The design leverages a modular 'block' design for capacity expansion and scales given the rate of customer onboarding. Subscribers must have a valid client access license (CAL) for the appropriate platform (either enterprise or standard) and a valid common access card (CAC).

Defense Connect Online (DCO)
Defense Connect Online (DCO) is the Department's designated enterprise tool for worldwide synchronous communication among national, Department of Defense, service, and non-governmental organizations. DCO provides its more-than 600,000 users instant messaging, persistent chat rooms, and web conferencing, which includes desktop and presentation sharing, audio and video conferences, and breakout sessions.

IdAM Portfolio and Enterprise Directory Services
This session will present an overview of DISA's Identity and Access Management portfolio. The presentation will include the mission overview, capabilities and strategic vision across the portfolio. Capabilities discussed during this session includes Enterprise Directory Services (EDS), Attribute Based Access Control (ABAC), and DoD Visitor.

Enterprise Services Track Schedule

Monday

2:30 p.m. – 4 p.m.	Enterprise Services Overview	Room 22/23

Tuesday

1:45 p.m. – 3:15 p.m.	IT Efficiencies	Room 22/23
3:30 p.m. – 5 p.m.	IdAM Portfolio and Enterprise Directory Services	Room 22/23

Wednesday

1 p.m. – 2 p.m.	DoD Enterprise Email Update	Room 22/23
2:30 p.m. – 3:30 p.m.	DoD Enterprise Portal Service	Room 22/23
4 p.m. – 5 p.m.	Defense Connect Online	Room 22/23

Identity and Access Management (IdAM)
The Identity Management Division (IA4) provides secure and reliable identity management services for DoD applications and systems. Services include identification, authentication, authorization, encryption, digital signature, integrity, and biometrics for consumers (e.g., business processes, applications, users) to support the Global Information Grid Enterprise Service; design, build, integrate, implement, and sustain the DoD Public Key Infrastructure (PKI), DISA Enterprise Directory Service - GDS and JEDS, and other identify management services as they are defined.

DISA Computer Network Defense Service Provider (CNDSP) Services
DISA is one of 23 accredited computer network defense service providers (CNDSP). DISA provides protect, detect, respond functions for all but two combatant commands (COCOM), all DISA entities and 12 DoD agencies/ field activities around the globe. This briefing will identify the detailed services customers can expect if aligned to DISA for CNDSP and how DISA is striving to improve and expand its CNDSP services.

Operationally-Focused Cyber Training Framework
Today's cyber operations are complex and unpredictable. Training is a key element for mission assurance. There are significant challenges to ensure our cyber workforce has both the capability and capacity to conduct operations in the cyberspace domain. This briefing will discuss the concept of providing a "Training Strategy Roadmap" for role-based and crew certifications.

Computer Network Defense (CND) Solutions [*FOUO*]*
Preparing for New Data Sources for CND
The DISA IA33 Sensor Grid branch has developed a new process that defines the steps necessary to establish and manage the architecting and implementation of new security monitoring capabilities. Determining where to start when analyzing new CND data sources is often challenging to manage because they involve a variety of technology solutions within different network boundaries that have distinct threat vectors. The lack of standard solutions for security monitoring and the evolving threat landscape make development of requirements particularly challenging. DISA IA33 has developed some basic guidelines to aid teams strategizing in the development of security monitoring solutions when introducing new data feeds.

Cyber Lumberjacking - Making the Most of Your Logs
Log management is needed by both security and operations for event monitoring of a common set of applications and information technology (IT) infrastructure. DISA is implementing an enterprise-level shared log management infrastructure to collect and store log events and to provide the capability to query log data and report for IT security. The need to collect, store, and analyze event information that is logged by data sources (network devices, servers, applications, database management systems, and storage) is driven by the Computer Network Defense mission. The log management infrastructure should be flexible to allow for data flows to be fed from a diverse set of IT security tools as security use cases such as targeted attack discovery require very broad monitoring of resources. The deployment of enterprise services provides a number of opportunities and challenges regarding security and monitoring of these new services. This briefing will focus on the first of these services: DoD Enterprise Email. We'll examine the architecture, available data, and Computer Network Defense use cases.

Enclave Versus Enterprise Analytics
The Joint Enterprise Email Security Gateway (JEEMSG) system will provide protection from internet-sourced email attacks for Defense Information System Network (DISN) enclave-level domains to include DoD combatant commands (COCOMs), military services, and agencies (CC/S/As). The JEEMSG system will serve as the first layer of defense to protect the DISN email domains from spam, malware, viruses, and prohibited content, but is not intended to replace existing enclave-level email security systems.

Enterprise Email Security Gateway
The JEEMSG system will process all email messages to and from enclaves eliminating the exposure to direct connections with Internet threats. Messages detected as spam and malicious are blocked and/or quarantined based on pre-defined policies directed by U.S. Cyber Command. Messages that are considered as potential spam or as a threat will be tagged to alert the enclave administrator, allowing them to take the final action.

**Government attendees and DISA contractors with a need to know ONLY. Additional badging required (CAC for government attendees and CAC with DISA ID badge for DISA contractors).*

Enclave Security
HBSS
The Host-Based Security Portfolio includes DISA tools that are designed to protect end points. Learn more about the current state of these tools (HBSS, AV/AS, wireless security, and bootable media) and future initiatives and activities, such as training, information sharing, new releases and more.

Secure Configuration Management
The Secure Configuration Management (SCM) session will provide information about the integration and optimization of enterprise information assurance (IA) applications and tools that use standardized data specifications and communication services to provide an automated and continuous process for security-focused configuration management. Attendees will learn about current and planned SCM capabilities available to all CC/S/A's.

Enhancing Cybersecurity
The Enterprise Connection Division will provide a comprehensive overview on how the combined actions of the Defense Security and Accreditation Working Group (DSAWG); Ports, Protocols, and Services Management (PPSM); and Information Assurance (IA) Branch collectively support DoD executive risk management assessments, DoD security and interoperability, and DISN configuration management and connection approval, providing essential added value to DoD's and DISA's cybersecurity efforts.

Cybersecurity Track Schedule

Monday

2:30 p.m. – 4 p.m.	DISA Computer Network Defense Service Provider (CNDSP) Services	Room 20/21

Tuesday

1:45 p.m. – 3:15 p.m.	CND Solutions [*FOUO*]*	Room 20/21
3:30 p.m. – 5 p.m.	Enclave Security	Room 20/21

Wednesday

1 p.m. – 2 p.m.	Enhancing Cybersecurity	Room 20/21
2:30 p.m. – 3:30 p.m.	Identity and Access Management	Room 20/21
4 p.m. – 5 p.m.	Operationally-Focused Cyber Training Framework	Room 20/21

**Government attendees and DISA contractors with a need to know ONLY. Additional badging required (CAC for government attendees and CAC with DISA ID badge for DISA contractors).*

State of C2 Evolution
The Joint C2 Objective Architecture is a key strategic enabler for evolving the Joint C2 capability area. It provides a technical framework to enable joint C2 capabilities to independently develop interoperable joint C2 services, systems, and data structures and exploit DoD Information Enterprise capabilities. It provides the implementation principles and constraints necessary to enable capability investment and modernization planning to achieve the DoD Information Enterprise Architecture (IEA) goals. This presentation will provide an update on the current state of the architecture and its implementation. Additionally, the Joint C2 capability area continues to evolve to provide more synchronized and consistent capabilities vice development of stovepipe systems within each of the DoD components. This presentation will provide an update on the concepts being used to drive this evolution as well as the status of a variety of key initiatives.

Joint C2: Situational Awareness and Intel (GCCS-J)
Global Command and Control System-Joint (GCCS-J) is the Department's Joint Command and Control (C2) system of record and an essential component for successful implementation of the operational concepts of dominant maneuver, precision engagement, and full-dimension protection. GCCS-J provides the foundation for migration of service-unique C2 systems into a joint, interoperable environment. GCCS-J provides a fused picture of the battlespace within a modern command, control, communications and computer system that is capable of meeting joint warfighter needs. GCCS-J incorporates the core planning and assessment tools required by combatant commanders and their subordinate Joint Task Force commanders while meeting the readiness support requirements of the military services. To achieve this, GCCS-J provides situational awareness, imagery exploitation, indications and warning, collaborative planning, course-of-action development, intelligence mission support, and real-time combat execution capabilities needed to accelerate operational tempo and conduct successful military operations in the modern warfare environment.

Multinational Information Sharing (MNIS)
The presentation includes an overview of the multinational information sharing (MNIS) portfolio and a discussion of recent changes. The discussion will address how MNIS is leveraging partnership relationships within DISA to deliver the DoD Enterprise for U.S. and coalition warfighters, and to provide updates to changes to sponsor and stakeholder relationships. Unclassified information sharing discussions will focus on the extended enterprise to include non-government and private organizations in a non .mil environment required by combatant commanders to coordinate response efforts during humanitarian assistance/disaster relief and stability operations. Several capabilities are in place and there is a desire to field an enterprise solution with a common look and feel across combatant commands (COCOMs). This block will provide a status update of this effort.

Joint C2 Planning & Execution (JPES) and Combat Support (GCSS-J)
The key focus of the Joint Planning & Execution Services (JPES) discussion is its framework (JFW). The JPES Framework (JFW) is an essential infrastructure component within the JPES portfolio of capabilities and has applicability to the greater Adaptive Planning & Execution (APEX) community. JFW is designed to provide common services, such as a Joint Permissions Manager, which is a hybrid of role-based access control to satisfy legacy user access policies, and attribute-based access control, which allows applications to control user access based on user attributes. Additionally, JFW provides a Data Virtualization Layer that enables JPES to fully implement a net-centric construct, and move C2 joint planning capabilities into a service-oriented architecture environment through the modernization of legacy databases, by isolating the applications from hard-coded interfaces to the databases. JFW also provides an in-memory data cache solution to allow enhanced application performance. An overview of JFW will be provided in this session, illustrating current capabilities and future enhancements.

The Global Combat Support System-Joint (GCSS-J) is an information technology (IT) application that continues to implement the tenets of a service-oriented architecture to deliver visibility of combat support (CS) capability to the joint logistician (i.e., essential capabilities, functions, activities, and tasks necessary to sustain all elements of operating forces in theater at all levels), facilitating information interoperability across and between CS and C2 functions. In conjunction with other Global Information Grid (GIG) elements including GCCS-J, Defense Information System Network, Defense Message System, Computing Services, and combatant commands/military services/agencies' information architectures, GCSS-J will provide the IT capabilities required to move and sustain joint forces throughout the spectrum of military operations.

Achieving Mission Success and Efficiencies through Enterprise Cross Domain Services (CDS) and Security Assessment Standardization
Cross Domain (CD) technologies enable trusted information sharing between security domains and across the cyber plane. The Unified Cross Domain Management Office (UCDMO) is the central "knowledge broker," focusing on pertinent CD governance, reciprocity, capabilities, and risk challenges. This overview outlines our re-focused mission and operational objectives, with emphasis on enterprise CD services DoD-wide. In addition, it will provide an overview of the cross domain portfolio and baseline processes, to include process descriptions, uses, roles, and responsibilities. Cross Domain Overlay will be discussed, in the context of of CDS development and security assessment activities IAW NIST SP 800-53 and CNSSI 1253, including overlay contents, security control selection, and the development of additional CDS-related guidance and intent for each selected control.

DISA Audits and Transparency [*FOUO*]*
During this session attendees will obtain an understanding of how auditing an organization (particularly a Defense Working Capital Fund organization) provides better transparency for customers and accuracy for setting rates.

C2 and Info Sharing Track Schedule

Monday

2:30 p.m. – 4 p.m.	State of C2 Evolution	Room 10/11

Tuesday

1:45 p.m. – 3:15 p.m.	Joint C2: Situational Awareness and Intel (GCCS-J)	Room 10/11
3:30 p.m. – 5 p.m.	Multinational Information Sharing (MNIS)	Room 10/11

Wednesday

1 p.m. – 2 p.m.	Joint C2 Planning & Execution (JPES) and Combat Support (GCSS-J)	Room 10/11
2:30 p.m. – 3:30 p.m.	Achieving Mission Success and Efficiencies through Enterprise Cross Domain Services and Security Assessment Standardization	Room 10/11
4 p.m. – 5 p.m.	DISA Audits and Transparency [*FOUO*]*	Room 10/11

**Government attendees and DISA contractors with a need to know ONLY. Additional badging required (CAC for government attendees and CAC with DISA ID badge for DISA contractors).*

Engineering Unified NetOps for the Defense Information Enterprise
DISA's Service Assurance Framework (SAF) and NetOps Integration Framework (NIF) initiatives prescribe and facilitate the engineering of NetOps into all the services carried over the enterprise infrastructure that DISA is tasked to operate and assure, and into all of the underlying resources comprising that infrastructure. The SAF encompasses the entire service delivery lifecycle, ensuring that NetOps capabilities are integral to service development and delivery. The NIF optimizes the architecture, standards, technologies, and tools used to provide operational capabilities to DISA and DoD NetOps personnel and organizations, ensuring both mission effectiveness and enterprise efficiency. This session will outline the SAF and NIF and describe how the NetOps Program Management Office – in collaboration with all of the DISA NetOps capability providers, Global Information Grid Operations (GO), DoD Enterprise Email (EE), and the Information Technology Service Management Office (ITSMO) – directly support the goals of Unified NetOps for the Defense Information Environment and synergize with DISA's Operational Framework.

DISA's Operational Framework in Support of Mission Partners
DISA's Operational Framework provides the context for how DISA operates and assures a reliable, available, secure and protected global net-centric enterprise across the full spectrum of military requirements. This briefing provides an overview of the agency's design and organization for executing NetOps, discusses how we interact with our mission partners, and explores the way ahead for the future.

Panel: Mission Partner Workflow Integration for the Enterprise Service Support Model
This is a joint brief/panel session with Information Technology Service Management Office (ITSMO), Enterprise Services Directorate (ESD), Global Information Grid Operations (GO), Program Executive Office-Mission Assurance, and Army.
This session will provide an understanding about what to expect when becoming a subscriber of an enterprise service. It will describe how enterprise services are supported in both the mission partner environment and DISA, with the idea of getting understanding into the field about what to expect when an organization becomes a user of DoD Enterprise Email, Defense Portal Service, etc.

Cyber Situational Awareness
The primary purpose of cyber situational awareness (SA) is to give decision makers and warfighters complete, accurate, and timely information about the enterprise infrastructure and the services available over it to enhance mission assurance. Cyber SA is produced through common processes, standards, and instrumentation, enabling near-real-time manipulation of any cyber asset to optimize the performance of our cyber capabilities and maximize our ability to operate in cyberspace as necessary. Every functional element of NetOps contributes to delivering effective cyber SA: enterprise management, content management, and net assurance. This session will explain the NetOps mechanisms used to produce cyber SA and some of the major tools that will be used for that purpose in the Defense Information Enterprise: Global NetOps Information Sharing Environment (GNISE), Mission Assurance Decision Support System (MADSS), Joint Incident Management System (JIMS), Community Data Center (CDC), and more.

Supporting Mission Partner OPLANS
DISA's Readiness program takes in the full spectrum of engineering, command and control capabilities and enterprise infrastructure to continuously operate and assure a global net-centric enterprise in direct support to warfighters, national-level leaders, and mission partners. This session provides a forum to explore the interdisciplinary nature of sustaining DISA and military readiness as it relates to command, control, communications, comuters, and intelligence (C4I) capabilities including our assessment of mission essential tasks and critical infrastructure as they relate to CCDR's OPLANS.

Emerging NetOps Capabilities
This session will cover integrated satellite communications (SATCOM) Operations and Management (ISOM)/ Integrated Transport Operations and Management (ITOM) and Service Quality Managment/Service Assurance and Information Sharing.

Network Operations Track Schedule

Monday

2:30 p.m. – 4 p.m.	Engineering Unified NetOps for the Defense Information Environment	Room 15/16

Tuesday

1:45 p.m. – 3:15 p.m.	DISA's Operational Framework in Support of Mission Partners	Room 15/16
3:30 p.m. – 5 p.m.	Panel: Mission Partner Workflow Integration for the Enterprise Service Support Model	Room 15/16

Wednesday

1 p.m. – 2 p.m.	Cyber SA	Room 15/16
2:30 p.m. – 3:30 p.m.	Emerging NetOps Capabilities	Room 15/16
4 p.m. – 5 p.m.	Supporting Mission Partner OPLANS	Room 15/16

Enabling the Enterprise with Efficient Use of the Spectrum
The Department's requirement for real-time information is constantly increasing. Better real-time situational awareness information leads to better decisions that increase the likelihood of mission success. In a tactical environment as well as operations other than war, the information transport medium of choice is wireless, which requires spectrum access. As the Department's demand for information grows, so does it's spectrum access requirements. Concurrently, the private sector and other government users demand for spectrum access has grown exponentially as well. Since the radio frequency spectrum is a limited resource, DoD must be proactive in planning for its future use of the spectrum. This track session will include two panel discussions — "DoD Spectrum Strategy" and "Spectrum Impact on Operations." The Strategy Panel will focus on why spectrum is important to DoD, the challenges DoD faces, and how it is planning for its future use of the spectrum. The "Spectrum Impact on Operations" session will focus on ensuring operational freedom of maneuver within the Electromagnetic Spectrum.

DoD Open Source and Community Source Software Development in Forge.mil
For several years now, the DoD CIO has been a proponent for the use of open source and community source software. Forge.mil was initiated almost three years ago to support that, and in fact is a service that's built upon open source software. With more than 14,000 registered users and 700 projects, Forge.mil is providing tangible value to the Department by allowing others to download software releases and other software development artifacts at no cost; and to leverage its application lifecycle management and collaboration tools as well as the emerging integration with cloud enabled infrastructures and continuous delivery processes. This is an overview of the capability of Forge.mil, how it facilitates open source software, and the relationship between Forge.mil, the RACE cloud, Continuous Integration processes, and the Continuous Delivery Platform initiatives.

How to Fill Technology Gaps in DoD
Based on the analysis done on technology gaps within DISA, Chief Technology Office is determined to find a way to bridge those gaps. This briefing will identify these capability gaps based on this analysis and demonstrate current and future initiatives that will further eliminate technology gaps within the agency.

DoD ESI & The Joint Information Environment (JIE)
DoD goals for increasing operational effectiveness while reducing information technology (IT) infrastructure costs are driving the construct of operational models to bring greater efficiency to the acquisition of commercial off-the-shelf (COTS) IT products and services. This session provides an overview of how DoD ESI supports the acquisition of enterprise COTS IT, with emphasis on its contributions to the JIE and the underlying IT Enterprise Strategy & Roadmap (ITES&R). Discussion will focus on: 1) Commodity software and IT hardware acquisition – how DoD ESI leverages component expertise to create enterprise agreements which capitalize on the economies of scale of the DoD for low prices and DoD preferred terms and conditions; 2) DoD ESI's role in the ITES&R and the JIE, and how JIE will be developing and enforcing IT software and commodity IT hardware acquisition processes; and 3) best value toolkit for IT buyers – DoD ESI-developed templates and training materials for IT buyers to estimate the total cost of ownership and evaluate investment alternatives.

DoD ESI is the joint DoD project to develop and implement a DoD enterprise-wide IT Asset Management (ITAM) process. The objectives are to save money and improve information sharing. ESI's focus is primarily on COTS IT products.

How DoD leverages Emerging Technologies
This session will cover how DISA and DoD exploit emerging and mature technologies to introduce new operational solutions to solve important military problems. These efforts facilitate transition of these technologies from developers to users while filling gaps on the Global Information Grid (GIG) to achieve Net Centric Operations. Topics of discussion include the Joint Capability Technology Demonstrations (JCTDs) process, COCOM emerging requirements, and upcoming technologies.

Strengthening Technology Investments through DISA Partnerships
This session will expose DISA mission areas and partners to the value of Technology Transfer, Cooperative Research and Development Agreements (CRADAs) and other T2 mechanisms which promote commercialization; the benefits of reduced time, cost, and risk of R&D projects; strategies and opportunities for linking mission needs with marketplace capabilities; and the economic and societal impacts from leveraging R&D investments by exploring innovative approaches to technical solutions and increased use of federal technologies by the private sector industry, academia, State and Local governments.

Spectrum & Technology Topics Track Schedule

Monday

2:30 p.m. – 4 p.m.	DoD ESI & The Joint Information Environment	Room 13/14

Tuesday

1:45 p.m. – 3:15 p.m.	Enabling the Enterprise with Efficient Use of the Spectrum	Room 13/14
3:30 p.m. – 5 p.m.	How DoD Leverages Emerging Technologies	Room 13/14

Wednesday

1 p.m. – 2 p.m.	DoD Open Source and Community Source Software Development in Forge.mil	Room 13/14
2:30 p.m. – 3:30 p.m.	How to Fill Technology Gaps in DoD	Room 13/14
4 p.m. – 5 p.m.	Strengthening Technology Investments through DISA Partnerships	Room 13/14

Overview of Testing & Evaluation for Enterprise Capabilities
DISA Testing and Evaluation (T&E) is evolving from traditional test methodologies to an Enterprise Services Test and Evaluation approach. This session will include an overview of DISA's T&E strategy for Enterprise Services to support autonomous T&E of services and new suitability and user experience challenges. Then, a specific example will be introduced, DISA's T&E Approach for Mobility, with discussions ranging from devices to applications.

Confidence in Scalability
Evaluating scalability for Enterprise Services is a challenge that DISA T&E is taking major strides to address. After an overview of the new evaluation criteria being developed to ensure scalability and total cost of ownership, we will present detailed examinations of scalability test efforts for a DISA service, Enterprise Mission Assurance Support Service (EMASS), and a U.S. Transportation Command (TRANSCOM) service, Rapid Development and Sustainment of Enterprise Mission Services (RDEMS).

Testing within an Enterprise
DISA Testing and Evaluation (T&E) is undergoing a major effort to reengineer the test environment for Enterprise Services. A series of presentations will describe the Federated, Pre-Production Environment in which Enterprise Services will be hosted, software tools that will be developed and provided to programs and testers, details on how virtualization will be used for autonomous automatic testing, and a description of test military service mission threads across the Enterprise.

Certifying Interoperability of an Enterprise
This session consists of a DoD CIO overview of interoperability certification and what to expect with oversight transition from Joint Staff to CIO, followed by a Joint Interoperability Test Command (JITC) presentation on the changes being made to better integrate with DoD programs and other test agencies to increase reciprocity in testing.

Testing Commercial Enterprise Services
This session will address the latest developments in testing of services from the perspectives of industry and academia. Dr. Bart Dahmer will discuss the FedEx test process and how they develop and field capabilities across their Enterprise. Dr. James Hill, Indiana University-Purdue University Indianapolis, will address recent research on techniques for evaluating and validating quality-of-service properties of enterprise-distributed systems continuously throughout the software lifecycle.

The Role of Test in a DevOps World
DevOps is the integration of software development with IT operations to enable the rapid delivery of new capabilities, and automated testing is a lynchpin necessary to make this happen. The role of Test needs to evolve to support this constant motion, and in the end will provide better, faster, more comprehensive coverage than traditional "over the fence" approaches. This brief provides examples (positive and negative) from real programs of record to show how Test integrates in a DevOps flow, and how the capabilities of Forge.mil support this role.

Testing Track Schedule

Monday

2:30 p.m. – 4 p.m.	Overview of T&E for Enterprise Capabilities	Room 18/19

Tuesday

1:45 p.m. – 3:15 p.m.	Confidence in Scalability	Room 18/19
3:30 p.m. – 5 p.m.	Testing within an Enterprise	Room 18/19

Wednesday

1 p.m. – 2 p.m.	Certifying Interoperability of an Enterprise	Room 18/19
2:30 p.m. – 3:30 p.m.	Testing Commercial Enterprise Services	Room 18/19
4 p.m. – 5 p.m.	The Role of Test in a DevOps World	Room 18/19

DISA/DITCO Procurement Support to DoD
This session will entail a discussion of the resources available to DISA and its mission partners covering a wide variety of existing contracts for telecommunications and information technology products and services; assistance with acquisition packages including complex documentation such as acquisition plans, justification(s) and approval(s); new focus areas/initiatives such as small business set-asides within existing multiple award contracts, increased communication with industry partners (requests for information, advisory multi-step process, industry days, presolicitation/preproposal conferences); mini-tutorials on enhancing competition via performance-based work statements, use of oral discussions, plus guidance for composing defensible sole source justifications.

Small Business Set-Asides for Multiple Award Contracts plus Ordering Guide Changes
This session will address significant changes in terms of how DISA can reach small businesses, including the new parity policy as well as current and pending changes to the way our mission partners need to build their requirements packages. Pending DARS changes will also be highlighted, namely LPTA, as well as new guidance on FAR Parts 8/16 procurements.

DISN Requirements Convergence to Support Unified Capabilities
DISA's convergence to support enterprise services and unified capabilities extends to the revised Capabilities Production Document (CPD) for the Defense Information System Network (DISN), and the way that DISA is considering contracting for networking services beyond the DISN Core. DISA is moving away from circuit-oriented contracting. This presentation will discuss how the DISN is moving towards a highly-meshed Internet Protocol (IP) router solution more suited for unified capabilities solutions for both its internal circuits used for DISN access/ selected DISN Backbone needs, and to satisfy customer-meshed circuit needs where use of the DISN core is not called for. This session will examine how the CPD and the Global Networking Services (GNS) Capabilities Need Document (CND) are evolving, and will point to social media sites that allow for government input on both documents, and industry input for the CND.

Unified Capabilities Requirements: UCR 2013 and DoD UC APL
This session will provide an overview of OSD Unified Capabilities Requirements document and planned changes for the next revision entitled UCR 2013. Key changes that will be discussed include new product categories, terminology changes, document size reductions, and future requirements. Finally, a high-level schedule and milestones for UCR 2013 will be covered.

The second portion of the session will focus on the Unified Capabilities Certification Office (UCCO) and how DISA manages the Approved Products List (APL). In accordance with DoD Instruction 8100.04, the APL is the only listing of UC equipment by DoD to be fielded in DoD networks. DoD components are required to fulfill their UC system needs by only purchasing APL listed products. This session covers the process for how DoD customers can find and locate products on the APL to meet their requirements. Additionally, the session will explain the process for vendors finding DoD sponsors in order to take their products through testing and certification so the products can be added to the APL.

Internet Protocol Version 6 (IPv6)
The IPv6 Transition effort consists of all of the activities required to upgrade the agency's Internet Protocol standard from IPv4 to IPv6. These requirements are defined and mandated by OMB and DoD policy and guidance.

DISA Enterprise Service Management Framework
DISA Enterprise Service Management Framework (DESMF) draft was released by the Information Technology Service Management Office (ITSMO) Feb. 1, 2012. This draft document focuses on defining a single service management framework that includes practices, outlines the supporting processes and details the goals, outcomes, and interfaces for these processes. It incorporates the complexities of ITIL/ITSM, interweaving other standards and best practices and provides the structure, stability, and strength to service management capabilities with durable principles to facilitate the management of Enterprise Services.

Virtual Small Business vs. Traditional Small Business: Tweets, Texts, Tools, and Trends
This track session is for small business only. The DISA Office of Small Business Programs will host an engaging session on technological trends in the federal marketplace.

DoD Cyber IA Range
The DoD Information Assurance Range provides a capability to support cyber-based exercises, training, and testing of IA/CND capabilities in an operationally realistic environment representative of the Global Information Grid. This brief will provide an overview of the DoD IA Range and information on how customers can leverage its capabilities.

HBSS Training
Host Intrusion Prevention 8.0 Migration Tool
This demonstration will be focused on the operation of the HIPS 8.0 Migration Tool. The demonstration will explain why the tool is needed as well as lessons learned around best practice for using the tool. The audience will see a migration from HIPS 7.0 policy to HIPS 8.0 Policy from start to finish. After viewing the demonstration, the audience will have a firm understanding of the need for the tool as well as how it operates.

Policy Auditor 6.0
This demonstration will be focused on the usage of PA 6.0 to audit systems within DoD. The demonstration will utilize the STIG Benchmarks to create an audit and then review the audit scores returned by the endpoint. The audience will experience the process of activating benchmarks, creating audits, and viewing the audit results.

Special Sessions

Tuesday

1:45 p.m. – 3:15 p.m.	DISA/DITCO Procurement Support to DoD	Ballroom C
3:30 p.m. – 5 p.m.	Virtual Small Business vs. Traditional Small Business: Tweets, Texts, Tools, and Trends	Ballroom B
	DISN Requirements Convergence to Support Unified Capabilities	Ballroom C

Wednesday

1 p.m. – 2 p.m.	DISA Enterprise Service Management Framework (DESMF)	Ballroom B
	DoD Cyber IA Range	Marriott Room 12
	Unified Capabilities Requirements: UCR 2013 and DoD UC APL	Ballroom C
1 p.m. – 3 p.m.	HBSS Training: Host Intrusion Prevention 8.0 Migration Tool	Marriott Room 11
2:30 p.m. – 3:30 p.m.	Internet Protocol version 6 (IPv6)	Ballroom B
	Small Business Set-Asides for MACs & Ordering Guide Changes	Ballroom C
3 p.m. – 5 p.m.	HBSS Training: Policy Auditor 6.0	Marriott Room 11

Description
DISA is committed to enhancing current capabilities, leveraging mobile technology, adapting it to the Defense environment, and ensuring that there is a strategy in place to take advantage of emerging technologies .

Objectives
DoD and DISA seek to develop common sense policies and procedures that enable the secure/assured and effective use of commercial mobile technologies without endangering the network. Operationally, DISA must enable services for the edge: any user, any device, anywhere – to include mobile users.

Challenges
The ability to economically leverage the commercial carrier architecture while assuring the transmission of unclassified applications, voice, and data is a daunting task. A second task will include expanding the service to include classified applications, data, and voice. Security and management to assure and secure mobile applications, voice, and data anywhere in the world are the greatest challenges to delivering mobile computing services at the enterprise-level. DoD and DISA are interested in partnership opportunities with commercial vendors.

Specific Challenges for Industry
- How can/does industry provide mobile computing services that meet the DoD's security and management requirements?
- How can industry assist DoD to economically leverage the commercial carrier architecture while assuring the transmission of voice and data unclassified applications?
- How can industry assist DoD to expand service to include classified data/voice applications?
- What specific DoD mobility requirements are generating the biggest cost drivers?

SESSIONS

DISA Overview: Mobility
This session will describe some technology (e.g., wireless/cellular/SATCOM) assessment and implementation activities that DISA and their mission partners have determined would be applicable to deployed or mobile users. One example is dismounted soldiers with portable devices (e.g., tablets, smartphones) wirelessly connected to deployed vehicles using SATCOM for connection to the Global Information Grid/Defense Information System Network (GIG/DISN) enterprise.

Industry Tracks

Accenture: *Always On, Always Connected. Keeping Up With Mobility in 2012*
Accenture's mobility track will be a fast-paced, highly interactive panel discussion with industry subject matter leaders focused on how to use, field, and secure mobile-device based solutions TODAY – not someday. The discussion will explore considerations and approaches in areas such as employee/contractor owned device use and associated management, with considerations around services an organization can provide and receive as managed services while maintaining the security of the mobile access, applications, and data. These topics will be examined from both an internal (operational) and external (end-user) viewpoint, bringing commercial perspectives into relevant DoD use cases that will also include an overview of many of the security and operational challenges to be managed. The three part track discussion will examine mobile device trends and Bring Your Own Device (BYOD), mobile application development and stores, and mobile security.
Session Executive: Dave Morales, Executive Vice President, Defense Technology Solutions, Accenture Federal Services
Moderator: Kyle Michl, Vice President, Defense Technology Solutions, Accenture Federal Services
Panelists:
- Roger Dunbar, Chairman of the Board, Silicon Valley Bank
- Soren Burkhart, Director, Accenture Mobility Services for Federal, State, Local, and Nonprofit
- Adrian Turner, CEO, Mocana Corporation
- Architecture/Infrastructure or Software Solutions Vendor TBD

AT&T: *Holistic Approach to Securing Mobility*
This session will cover the convergence of emerging technologies driving the move to mobility as well as presenting a holistic, layered vision of the architecture to truly secure mobile communications, processing, data storage, and data access leveraging the entire infrastructure from the mobile device through the network and to the data center. Trade-offs will be discussed and example solutions presented as to how this vision can be realized.
Speaker: Jack Golden, PE, CISSP, Technical Director, Secure Mobility Practice, AT&T Government Solutions

Unisys: *Achieving Mobility with Consumer Devices using Cloud Collaboration*
How can DoD and other Federal agencies use industry solutions to enhance end user productivity by delivering secure access to cloud based advanced collaboration tools on consumer mobile devices? Focusing on cloud email and collaboration services like Google Apps, learn about the integration of tools for secure authentication, access control, and device management to protect security-sensitive information. Hear about the experience to date with deployments in the federal government and for private sector customers with comparable unclassified security/assurance requirements. Participate in a discussion about how to extend existing solutions to address DoD mobility requirements while minimizing cost and maximizing the benefits from today's available cloud services and to set the stage for next-generation mobile enterprise applications with the convenience expected by the DoD user community.
Speakers:
- Mark Cohn, Unisys Federal Chief Technology Officer
- Steve Kousen, Vice President for End User Services

Harris: *Partnering to Provide Solutions Across the Entire Mobile Network*
As government mobile phone users continue to push the need for more applications over handheld devices, applications are playing a more important role than ever. What are some exciting examples of those applications and how they are being used by government users today? What are some of the challenges, issues and solutions to developing cost-effective mobile capabilities while remaining device agnostic? Industry leaders offer insights into providing this effective tool for the DoD while maintaining cost-effectiveness, security, portability and ease of use across universal mobile device platforms.
Moderator: David Cavossa, President, Government Solutions, Harris CapRock
Speakers:
- Tom Cox, President, Coolfire Solutions
- Ed Wright, Chief Operating Officer and Vice President for Business Development, U.S. Space Mobile Communications

Mobile Computing & Devices Track Schedule

Monday

2:30 p.m. – 4 p.m.	DISA Overview: Mobility	Room 7/8/9

Tuesday

1:45 p.m. – 3:15 p.m.	Accenture: Always On, Always Connected. Keeping Up with Mobility in 2012	Room 7/8/9
3:30 p.m. – 5 p.m.	AT&T: Holistic Approach to Securing Mobility	Room 7/8/9

Wednesday

1 p.m. – 2 p.m.	Unisys: Achieving Mobility with Consumer Devices Using Cloud Collaboration	Room 7/8/9
2:30 p.m. – 4 p.m.	Harris: Partnering to Provide Solutions Across the Entire Mobile Network	Room 7/8/9

Cloud Computing

Industry Presentations with DISA Overview

Description
Investments in IT will build upon a department-wide cloud platform that speeds and simplifies the acquisition and deployment of new functionality while minimizing costs. A DoD cloud is essential for the establishment of a joint enterprise information environment and the provision of defense enterprise services. We believe the DoD cloud will be a combination of governmental and private industry solutions. DISA is looking for opportunities to act as a cloud broker through which the services can contract cloud capabilities from a private vendor meeting our security and operational standards.

Objective
To gain the efficiencies a cloud infrastructure provides by supporting the development and execution of a strategy and standards for a secure DoD cloud environment.

Specific Challenges for Industry
- What are the greatest obstacles (e.g., acquisition and funding, cultural shift, trusting another organization to store and safeguard your data) to moving to a cloud environment and how can or have you overcome those challenges?
- What are business best practices and metrics for evaluating cloud computing capabilities?
- What are best practices for converting or sun setting applications to move to a cloud environment?
- How can industry meet the levels of security and NetOps required by the DoD private cloud?
- What would be your NetOps concept, i.e. would or how would users be informed of outages, length of outage, service impacts, etc.?
- What are some innovative concepts to support adopting commercial solutions, services, and/or materiel?
- How would you partner with DoD so network assurance and net defense capabilities are incorporated into your offerings?

SESSIONS

DISA Overview: Platform as a Service (PaaS) and RACE Overview
This session will define the services provided by DISA's Platform as a Service (PaaS) and Rapid Access Computing Environment (RACE) offerings. It will include definitions of the capabilities and support models, descriptions of the pricing models, and options available within the services. The session will end with an exercise of the development/release/decommissioning lifecycle of a sample web application using the RACE portal and PaaS capabilities.

Industry Tracks

Booz Allen Hamilton: *Cloud Services that Enable the Mission - Lessons Learned from the Trenches*
The potential of the cloud has many organizations thinking fundamentally differently about their infrastructure and data. Cloud services can more effectively enable the mission of today's warfighters; however, providing and using cloud services is a challenging prospect that requires the integration of multiple dimensions of cloud computing, regardless of the cloud provider or solution. When aligned correctly, these cloud dimensions can help organizations realize benefits of speed, simplification, and decreased costs. In this session, Booz Allen will share case study experiences from our vast portfolio of cloud engagements to address obstacles and strategies in moving to the cloud, determining how data can be secured across cloud environments, and providing lessons learned and the mission impact of successful cloud engagements.

SAIC: *Journey to Cloud Computing Presentation and Panel*
This session will describe the approaches, experience gained, and lessons learned from a multi-year investment in cloud computing for a corporate infrastructure project and subsequent solutions derived for the market. The presentations and panel discussion will highlight how government customers can benefit from industry's experience with cloud integration.
Moderator: Charles E. Beard, SAIC Senior Vice President, Chief Information Officer, and General Manager of Cybersecurity
Panelists:
- Peder J. Jungck, SAIC Senior Vice President and Chief Technology Officer Cybersecurity
- Robert R. (Bob) Logan, SAIC Vice President and IT Engineering Director
- Jonathan C. (Jon) Bollers, SAIC Vice President and Director of Technology Solutions, Corporate CTO
- Richard G. (Rick) Goodwin, SAIC Vice President and Business Unit Chief Scientist

HP: *Cloud Computing*
It's like a drumbeat for today's enterprise – managing complexity while faced with budget constraints. To overcome the challenges, the DoD is turning to the cloud – deploying public, private, community, or hybrid – to achieve greater cost savings and efficiencies. This aggressive market shift has early adopters of lightweight cloud capabilities rapidly moving into enterprise consumption of both public and private clouds to meet consumers' needs. What's next? How will DoD cloud models evolve into the future? How can the DoD be prepared to manage change within the enterprise? How must IT transition to be a broker of cloud services? As DoD transforms, controlling and pacing the cloud journey will help maintain operations and maximize investments. Understanding the evolution, then the impact to the enterprise, is critical for success.
Moderator: Steve Ressler, Founder and President of GovLoop.com
Panelists:
- Jeff Bergeron, HP Chief Technologist, US Public Sector
- Susie Adams, Microsoft, Chief Technology Officer, Federal

Juniper: *Mega Data Centers - The New Information Infrastructure*
Despite the overwhelming buzz created by cloud computing across the Federal landscape, these discussions generally focus on emerging cloud applications. There is a serious lack of "networking" conversation being had, as it's assumed that the cloud builder's network will always operate. But as agencies move more resources into the cloud, connectivity to and from it increasingly becomes an issue, especially in hybrid environments. Security, reliability, and performance should be at the top of mind. This session will discuss the technologies that can be deployed to address cloud infrastructure challenges and assure a secure, guaranteed experience for government agencies that rely on cloud resources. In particular, this talk will address the following specific challenges:
- Gain the efficiencies that a cloud infrastructure provides by supporting the development and execution of a strategy and standards for a secure DoD cloud environment.
- Bridging the divide that separates private, wholly owned data centers from public, capacity-for-hire cloud providers. The role for IT in creating a bridge across this divide as virtualization of all types enables more efficient application development, virtual machine provisioning and business continuity.
- What will it take to securely integrate on-premises infrastructure with that running in a public cloud provider?

Speaker: Dean Sheffield, Global Managing Director for Cloud Networking, Juniper Networks

BAE Systems: *A Practical Approach to Cloud Computing*
Many organizations are being faced with an increasing demand to move to a cloud platform for faster and simpler acquisition and deployment of new functionality while minimizing costs; but many of these organizations struggle with exactly how to make the move to a cloud platform. This session will provide attendees with the understanding of cloud, cloud architectures, cloud deployment models, ideas on how to move to the cloud, and real life lessons learned on implementing a cloud platform. The objective of this session is to present attendees with the understanding of what cloud infrastructure provides and how to formulate a strategy to move to a cloud environment.
Speaker: Mitch Daniels, Chief Engineer, Information Technology and Cybersecurity Solutions

Cloud Computing Track Schedule

Monday

2:30 p.m. – 4 p.m.	DISA Overview: Platform as a Service & RACE Overview	Ballroom A

Tuesday

1:45 p.m. - 3:15 p.m.	Booz Allen Hamilton: Cloud Services that Enable the Mission - Lessons Learned from the Trenches	Ballroom A
3:30 p.m. – 5 p.m.	SAIC: Journey to Cloud Computing Presentation and Panel	Ballroom A

Wednesday

1 p.m. – 2 p.m.	HP: Cloud Computing	Ballroom A
2:30 p.m. – 3:30 p.m.	Juniper: Mega Data Centers - The New Information Infrastructure	Ballroom A
4 p.m. – 5 p.m.	BAE Systems: A Practical Approach to Cloud Computing	Ballroom A

Description
Unified Capabilities solutions provide integrated voice, video, and/or data collaboration services transported securely across ubiquitous and highly available Internet Protocol (IP) network infrastructure, independent of technology, to deliver increased mission effectiveness for DoD components. To enhance the offering to the business, intelligence, and warfighting communities, these services will be integrated with available DoD enterprise solutions, such as directory services, web collaboration, and e-mail to maximize their utility consistent with commercial UC offerings.

Objective
In accordance with the DoD CIO UC Master Plan and the UC Requirements (UCR), the objective is to migrate DoD to an enterprise, interoperable, IP-based UC service that includes end-to-end security, shared situational awareness, and enhanced wired and wireless support to meet the mission needs of the DoD's increasingly mobile subscribers.

Challenges
The primary challenge is to develop, in collaboration with the military services and DoD CIO, an implementation plan for a DoD-wide, end-to-end deployment consistent with the UC Master Plan. Additional challenges will include establishing regional priorities, validating the UC operational framework, refining the NetOps concept of operations, testing and deploying UC pilots, and funding/acquiring/deploying/operating/sustaining the unclassified and classified enterprise UC while transitioning from legacy DoD voice and video solutions.

Specific Challenges for Industry
NetOps
- What are best practices for maintaining an operational picture of the network that contains various manufacturers' devices?
- What troubleshooting tools and practices should DoD be using and deploying on the UC network?
- UC offerings vary in capability and maturity. In a few cases, the solutions are well-integrated; in other cases, solutions offer limited integration or interoperability in a multi-vendor environment. How can we retain the feature-rich capabilities across multiple vendors' UC products?
- What is the minimum feature set that should be available between all voice, video, chat, and presence systems that will meet the needs of 80 percent of the user community?
- DoD is deploying a hybrid UC – a blend of on-premises and cloud UC functionality. What are the challenges in deploying this hybrid environment?
- DoD is a very large enterprise which will have a large scaling requirements for UC on a broad geographical spread and a wide range of requirements. How is industry addressing these requirements (for example, transferring user profile information to include identity and privileges to a mobile device)?
- What is the quickest way that DoD can bring sensitive, but unclassified DoD UC (voice, video, chat, presence) to our home smart devices?
- How would industry propose to meet DoD's increasing need for mobility, enabling seamless wireless and portable UC application delivery to strategic and warfighting users while meeting the stringent DoD requirements for information assurance?
- The DoD seeks to use common, enterprise-wide directory solutions to the maximum extent possible. What solutions could industry provide to assist DoD with moving towards a platform independent user experience that allows for a common user profile across multiple UC-enabled devices?
- What would industry suggest to assist DoD with expediting the procurement of IP-based UC solutions, thereby reducing the installed base of legacy telecommunications equipment?
- Where does industry believe that DoD's requirements for UC can better align with the commercial sector with respect to performance, security, and infrastructure requirements while still meeting the core tenants of the DoD mission?
- What strategies would industry suggest to allow DoD to efficiently sustain UC solutions, following initial deployment, in a DoD enterprise-wide manner?

SESSIONS

DISA Overview: DoD Unified Capabilities and Tactical Unified Capabilities Overview
This session will focus on unified capabilities (UC) and DISA as the Department's preferred UC transport provider for internet and commercial satellite connections for voice, video, and data on DoD networks. It highlights the merging of independent systems and promotes future strategies intended to drive a converged Global Information Grid (GIG) architecture. This broader, strategically aligned definition enables the realization of operational advantages of converging systems throughout the GIG to include applications, services, and data; communications; information assurance; NetOps and enterprise management; and computing infrastructure. This session will also focus on UC

supporting tactical and deployed users. It highlights the unique issues UC faces in the tactical environment in comparison to the strategic environment. An overview of testing that has been completed during JUICE exercises as well as future test plans will be discussed.

Industry Tracks

CenturyLink: *A Carrier's View of Unified Capabilities*
An expert panel will discuss how a converged IP network delivery architecture can provide secure scalable and customizable solutions across various vendor platforms and in a hybrid environment of cloud and hosted applications. Attendees will benefit from the session by exploring solutions that support voice, data, video, applications, email, and collaboration services for a large enterprise across a broad geographical scale whether accessed through fixed or mobile devices.
Moderator: Diana Gowen, Senior Vice President of Sales and General Manager, CenturyLink Government
Panelists:
- Dave Shacochis, Vice President, Global Public Sector, CenturyLink
- Mike Glenn, Director of Enterprise Technology Security, CenturyLink
- Azhar Mirza, Director of Enterprise Architecture, CenturyLink
- Shawn Carroll, Director of Engineering, CenturyLink Government

URS: *Simplifying the Journey to Unified Communications*
Join a panel of industry leading partners who will present and discuss progress, pitfalls, and lessons learned on the journey towards achieving unified capabilities as they relate to the needs of government, military and civilian organizations. This panel will consist of representatives from industry leaders including Microsoft, Verizon, and Juniper Networks, and will be moderated by Air Force Lt Gen (ret.) Michael Peterson, former chief information officer of the Air Force. We look forward to an informative and thought-provoking discussion as we share experiences and expectations on the journey to unified capabilities, while addressing the needs of the warfighter of the future.
Moderator: Michael Peterson, Vice President, Strategic Initiatives, URS
Panelists:
- Bill Shelton, Director, Federal Strategic Initiatives, Juniper Networks
- Martin Isaksen, DoD Chief Technology Officer, Microsoft
- Tim Stone, Principal UCC Consultant, Emerging Technology Solutions, Verizon
- IBM (invited)
- Polycom (invited)

CSC: *Federal UC Challenges*
The primary challenge is to deploy UC services within the federal government in an environment of decreasing IT expenditures and competing requirements between federal organizations while maintaining legacy services. What guidance, advice, and counsel can the OEMs, software vendors, and carriers provide to help or assist the federal government to move UC forward, especially as the technology advances? Questions that require answers include (but are not limited to) the following:
- Are there benefits to consolidating the federal (e.g., DoD, state, Department of Homeland Security, etc.) information assurance (IA) requirements, and policies for UC products? What are the other federal departments doing? What does industry foresee with the IA community as it deploys emerging solutions such as virtualization and cloud-based solutions?
- In a federal environment of diminishing IT budgets, where should the federal government focus their UC expenditures?
- Developing UC architectures for federal customers can take multiple years given the processes and diverse customer base. What UC technologies will become mainstream in FY 2017 and when should the federal government start the research and development to prepare for those technologies?
- Terms like *virtualization of solutions, cloud enabling, software, platform, UC as a service* have been bantered around. What are industry's plans for UC (including wireless integration) related to these terms?
- Is industry developing tools to automate the massive provisioning of customers and how can the federal government exploit the capability?
- Legacy product end-of-life and lack of circuit switched system/TDM administrators, in combination with the increased efficiencies for UC, are driving the business cases for moving away from TDM to IP. With the projected funding environment faced by federal agencies, are enterprise solutions, including the formation of consolidated data centers that offer a host of standardized services, the best approach for federal chief technology officers to pursue for UC?

(CSC: Federal UC Challenges continued)

Moderator: John O'Meally, Senior Project Manager, CSC
Speakers:
- Vico Loquercio, Vice President, Solution Architecture and Strategy, Avaya Government Solutions
- Bill Shelton, Director, Federal Strategic Initiatives, Juniper Systems
- Pete Babendreier, DoD Technical Solutions Architect, Cisco Systems
- Jim Donovan, Vice President Enterprise Product Management, Acme Packet
- Eugene Kohlmeier, Director, Government Technologies, Redcom Laboratories
- Timothy Stone, Principal UCC Consultant, Emerging Technology Solutions, Verizon
- Martin B. Isaksen, Chief Technology Officer, Microsoft DoD Federal
- Nokia-Siemens Networks (NSN) - TBD

Oracle: *Leveraging Internet Innovation to Empower the Warfighter*
DoD unified capabilities calls for the integration of standards-based communications and collaboration services to provide increased mission effectiveness to the warfighter. A key tenet of unified capabilities is to leverage commercial off-the-shelf technology to meet DoD's mission requirements. This makes good sense because the rate of innovation on the web and public Internet far outpaces what could be done by government alone. Oracle is a driving force for Internet innovation and works with the largest and most successful service providers worldwide. This session will focus on how to identify innovative solutions already proven in private and public sector environments that would be a good fit to leverage as DoD unified capabilities data services and collaboration.
Speakers:
- Doug Gallarda, Master Principal Sales Consultant, Oracle Communications
- Peter Walsh, Principal Sales Consultant, US Federal DoD Technology

CISCO Systems: *Unified Capabilities–Benefits of Best Practices*
DoD's subscribers are increasingly mobile, and this session will focus on migrating from legacy voice and video solutions to an interoperable, secure IP-based unified capabilities (UC) service that includes shared situational awareness and identifies regional priorities. Attendees will learn about how to best integrate these UC solutions, how to develop an implementation plan consistent with the UC Master Plan, and best practices for installing and creating a multi-vendor environment that will ensure reliability, availability, diversity, and security.
Speaker: Pete Babendreier, Technical Solutions Architect for the DoD, Cisco Systems

Unified Capabilities/Convergence Track Schedule

Monday

2:30 p.m. – 4 p.m.	DISA Overview: DoD Unified Capabilities and Tactical Unified Capabilities Overview	Ballroom D

Tuesday

1:45 p.m. – 3:15 p.m.	CenturyLink: A Carrier's View of Unified Capabilities	Ballroom D
3:30 p.m. – 5 p.m.	URS: Simplifying the Journey to Unified Communications	Ballroom D

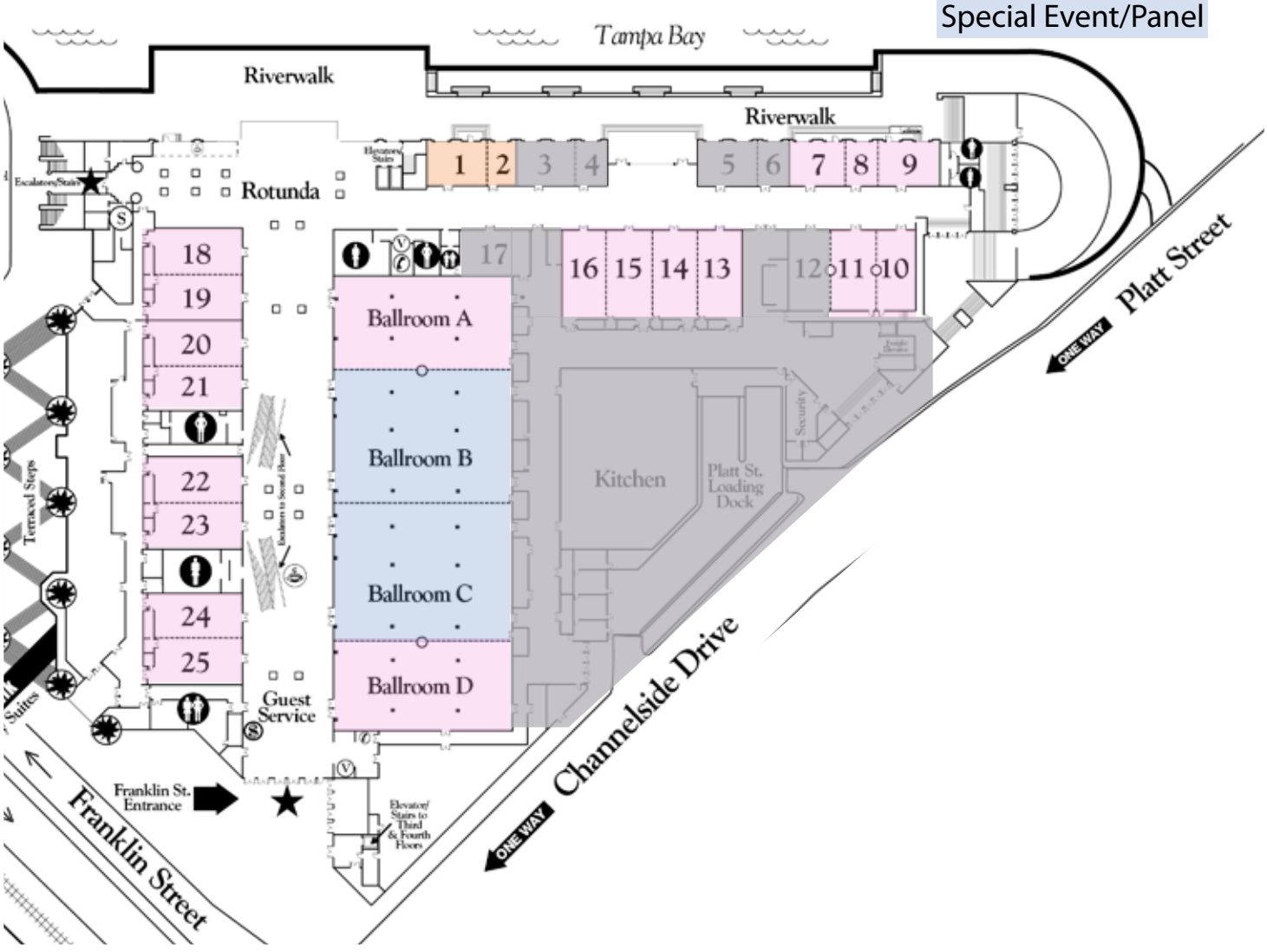
Wednesday

1 p.m. – 2 p.m.	CSC: Federal UC Challenges	Ballroom D
2 p.m. – 3:30 p.m.	Oracle: Leveraging Internet Innovation to Empower the Warfighter	Ballroom D
4 p.m. – 5 p.m.	CISCO Systems: Unified Capabilities - Benefits of Best Practices	Ballroom D

Tampa Convention Center

1st Floor

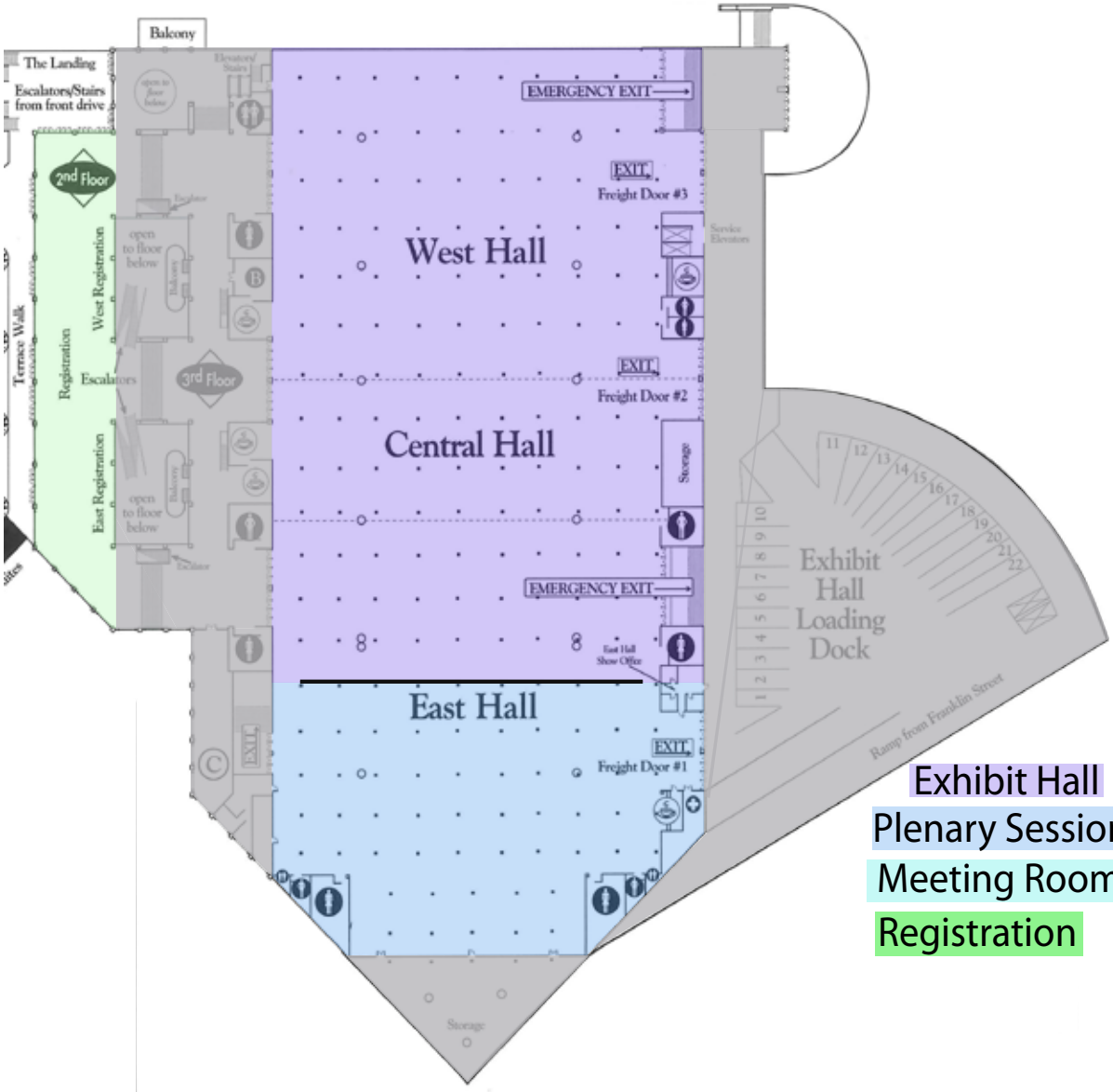
Track Rooms
DISA Ops Center
Special Event/Panel



2nd Floor

3rd Floor

4th Floor



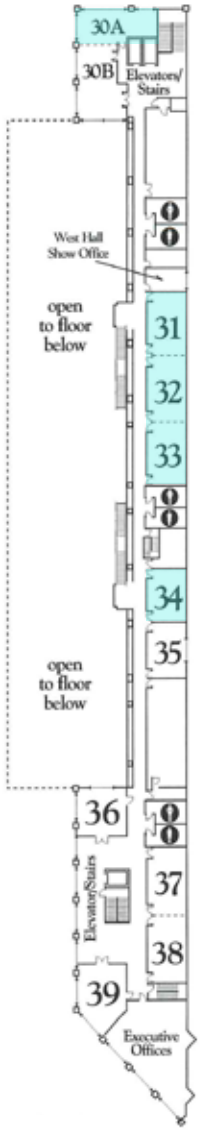


Exhibit Hall
Plenary Sessions
Meeting Rooms
Registration

DISA PAVILION EXHIBITS

827
TSEAS Inventory and Billing Information (TIBI)

823/825
DISA Chief Information Officer

1128/1131/1230/1231
DISA Forge.mil

1326/1324
Advanced Concepts & Experimentation

1330
DISA Technology Transfer

920
DISA Office of Small Business Programs

819
Defense Spectrum Organization
Global Electromagnetic Spectrum Information Systems (GEMSIS)

Tactical Operations Center
Net Ops
National Guard
Navy/Nav Air

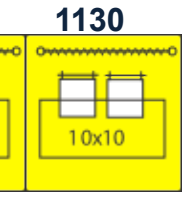
1322
Enterprise Software Initiative

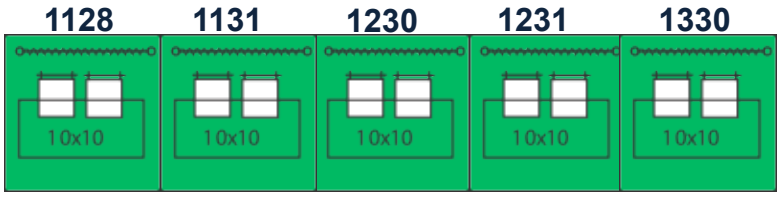
826/824/822/727/725/723
Enterprise Services Directorate

719/818
Field Security Operations (FSO)

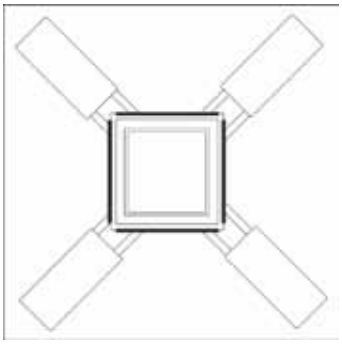
928/931/1030
Network Services Capabilities Center

DISA PAVILION EXHIBITS

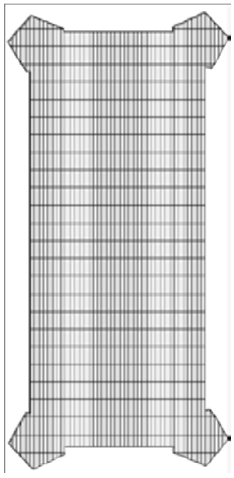


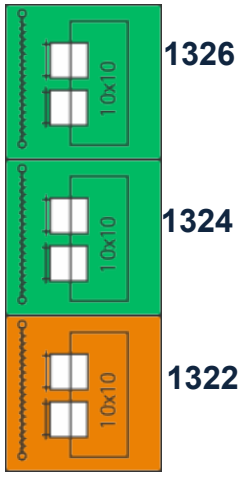


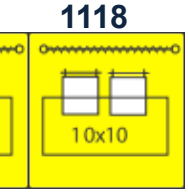
Tactical Operations Center

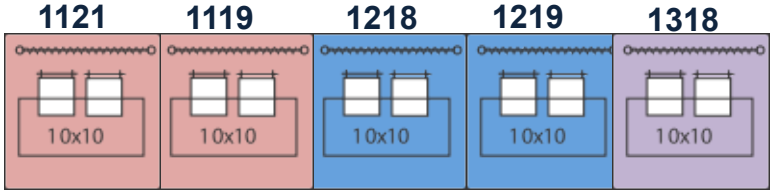


Drash Shelter









924/922
Network Services Customer Services

918/919
Network Services DISN Operational Support Systems

1031/1130
Network Services Enterprise Connection Division

926
Network Services Program Management Office

1018
Commercial Satellite Communications Center (FCSA/EMSS)

1019/1118
Program Executive Office for Communications (PEO COMMS)

731/830/831/930
Command and Control Capabilities

1218/1219
Program Executive Office- Mission Assurance Computer Network Defense Secure Configuration Management & Host Based Security

1318
DISA Employer of Choice

1121/1119
DISA Test and Evaluation

DISA CAMPAIGN PLAN 2013 - 2014

The DISA Campaign Plan is our roadmap for success. The plan defines our mission and vision, aligns our objectives with strategic goals, postures the agency to support the information technology (IT) needs of the Department of Defense (DoD), and is the mechanism by which the DISA vision is communicated to both our workforce and mission partners. It highlights our initiatives and guides the allocation of our resources and execution of critical investment decisions.

The Campaign Plan is organized into three Lines of Operation (Enterprise Infrastructure; Command and Control and Information Sharing; and Operate and Assure) and nine Joint Enablers (Acquisition; Contracting; Engineering; Information, Knowledge Management, and Process Improvement; People; Planning; Resources; Spectrum; and Testing). The Lines of Operation and Joint Enablers provide the framework for setting our priorities and describe the ways and means by which we will attain our strategic objectives.

As the goals of the Department evolve, we will adjust our course accordingly. The 2013 DISA Campaign Plan will place great emphasis on aligning with the Department's current vision of a secure, efficient, and effective joint information environment. The following goals will be the foundation upon which the Campaign Plan will be built.

GOAL 1

EVOLVE THE JOINT ENTERPRISE INFORMATION ENVIRONMENT.
Provide effective, reliable, robust capabilities where the user can connect with any device from anywhere on the globe and be productive. (Line of Operation 1)

GOAL 2

PROVIDE JOINT COMMAND AND CONTROL AND LEADERSHIP SUPPORT.
Engineer, provide and enhance command and control (C2) capabilities that allow mission partners to rapidly and effectively share real-time information across the strategic, operational, and tactical spectrum of operations. (Line of Operation 2)

GOAL 3

OPERATE AND ASSURE THE ENTERPRISE.
Strengthen network operations and cyber security by building and operating the enterprise as a single, well-defended enterprise infrastructure that more readily detects, identifies, responds, and quickly recovers from cyber threats and attacks. (Line of Operation 3)

GOAL 4

OPTIMIZE DEPARTMENT INVESTMENTS.
Enable the Department to maximize use of its resources by providing cost efficient capabilities; an effective and defensible physical infrastructure; standardized support services and business processes, and policies that enable the rapid infusion of technology. (All Lines of Operation & Joint Enablers)

The 2013 DISA Campaign Plan is planned for release in July 2012.

View the current DISA Campaign Plan at www.disa.mil/about/our-campaign-plan

About DISA

DISA MISSION PARTNER SERVICE PROVIDERS

DISA STRATEGIC BUSINESS UNITS

Network Services Directorate (NS), led by Cindy Moran

Consolidates all Defense Information System Network (DISN) activities under a single senior manager. Network Services translates customers' long-haul network requirements into effective voice, video and data network solutions; leverages proven and emerging technologies to ensure joint interoperability, assured security and best value; evaluates technical operations; and resolves technical support issues for DoD's long-haul networks. NS provides voice, video, data, transport, messaging, satellite, and wireless services.

Enterprise Services Directorate (ESD), led by Alfred Rivera

Delivers mature and standardized operations processes, centralized management, and partner-focused support. ESD manages all the partner data, including hardware components (computers, storage devices, and networks), software, and labor. ESD and Defense Enterprise Service Centers (formerly Defense Enterprise Computing Centers) provide the stable environment within which our partners' applications can run. Services included mainframe hosting, web hosting, server hosting and virtualization, application monitoring, and enterprise services (infrastructure, applications, and identity management).

Operations Directorate (GO), led by Larry Huffman

Coordinates and synchronizes DISA's "Operate and Assure" line of operation in support of the full spectrum of military requirements and operations and supports United States Cyber Command in its mission to provide secure, interoperable, and reliable operation of the Department of Defense (DoD) net-centric enterprise infrastructure. GO oversees the DISA field offices at each combatant command.

Enterprise Engineering Directorate (EE), led by Gerry Doyle

Provides a set of cross-program engineering services. These services are dedicated to solving problems that arise among different programs and projects where common solutions are needed to support joint interoperability. EE supports DoD-wide information technology standards development and configuration management as well as generating performance assessment models and simulations of both operational and planned network configurations.

ACQUISITION AND PROGRAM EXECUTIVE OFFICES

PEO for Command and Control Capabilities (PEO-C2C), led by Martin Gross

Provides executive lifecycle management of the command and control (C2) portfolio consisting of the programs, projects, and initiatives that support the joint warfighter plan and execute joint military and coalition operations. The PEO-C2C portfolio includes the Global Command and Control System – Joint, the Global Combat Support System – Joint, Multinational Information Sharing, and Joint Planning and Execution Services.

PEO for GIG Enterprise Services (PEO-GES), led by Alan Lewis

Provides portfolio management to develop, deliver, and support enterprise services for mission performance across the warfighter, business, and intelligence mission areas in support of the enterprise user vision.

PEO for Mission Assurance and Network Operations (PEO-MA), led by Mark Orndorff

Manages (acquires/develops, engineers, and implements) DoD information assurance and NetOps capabilities. PEO-MA provides responsive, secure, and interoperable net-centric solutions necessary to secure and operate the Global Information Grid.

PEO for Communications (PEO-Comms), led by Bruce Bennett

Provides acquisition oversight, program management, advocacy, and support for the satellite communications (SATCOM), teleport, and services portfolios.

Cross-Functional Solutions Directorate, led by Col David Stickley, USAF

Coordinates to ensure DoD IT effectiveness on an enterprise model and to integrate IT, intelligence, and business efficiency efforts. Near-term objectives are network normalization, identity management and access control, enterprise data center consolidation, enterprise services, and the Joint Information Environment implementation.

OTHER SERVICES

Procurement Directorate (PLD) and the Defense Information Technology Contracting Organization (DITCO), led by Kathleen Miller

Provides Enterprise Acquisition Services (EAS) for purchasing telecommunications and information technology (IT) products and services from the worldwide commercial sector to meet DoD and authorized non-defense customers' needs. Services include acquisition planning, procurement, tariff surveillance, cost and price analyses, and contract administration. DISA is the mandated single source for procuring DoD long-haul telecommunications requirements. PLD/DITCO also establishes large-contract vehicles available to DoD for essential IT services such as engineering, hardware, equipment and maintenance, integration and support, information security, computer technology, and Defense Information System Network (DISN) access.

Defense Spectrum Office (DSO), led by Stuart Timerman

Enables information dominance through effective spectrum operations. DSO provides commanders direct operational support, including electromagnetic battlespace planning, deconfliction, and joint spectrum interference resolution. DSO develops and implements net-centric enterprise spectrum management capabilities to enhance efficiency and effectiveness, and pursues emerging spectrum technologies that may either benefit or impact DoD's ability to access the electromagnetic spectrum. DSO advocates for current and future military spectrum requirements in national and international forums to protect DoD global operations.

Testing

The Office of the Test and Evaluation Executive (TEO), led by Luanne Overstreet, provides test and evaluation (T&E) oversight and guidance to DISA acquisition programs to ensure consistent application of sound T&E methodologies and processes.

The Joint Interoperability Test Command (JITC), led by COL Joseph F. Puett III, USA, is recognized throughout DoD and industry for their diligence in extensively testing and providing joint certification for the net-centric systems employed by our armed forces.

DISA SERVICE CATALOG

An updated version of the DISA Service Catalog is now available at **www.disa.mil**. This electronic version makes it easier to find and share information regarding all of DISA's service offerings, including rate/pricing information and ordering information.

The purpose of the Service Catalog is to provide an authoritative source of information regarding DISA's services and to ensure that the information is widely available to our mission partners.

The new version of the catalog includes an expansion of listed services that better represent DISA's full range of capabilities, informs our mission partners of the value our services afford, and provides situational awareness of services "in the pipeline." In addition, the Service Catalog users can now provide feedback to help us improve the quality of information available by clicking on the "Rate this Page" icon on the bottom-right side of each page.

The categories of services are listed below, and the colors of the icons show alignment of those services with the DISA's lines of operation and joint enablers as described in the DISA Campaign Plan.

DISA CAMPAIGN PLAN LINE OF OPERATION:
ENTERPRISE INFRASTRUCTURE

Enterprise Services
Network Services
Computing

DISA CAMPAIGN PLAN LINE OF OPERATION:
COMMAND & CONTROL AND INFORMATION SHARING

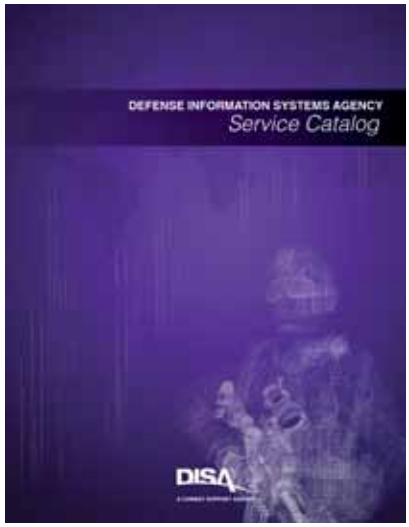
DISA CAMPAIGN PLAN LINE OF OPERATION:
OPERATE AND ASSURE

DISA CAMPAIGN PLAN JOINT ENABLER:
CONTRACTING

DISA CAMPAIGN PLAN JOINT ENABLER:
ENGINEERING

DISA CAMPAIGN PLAN JOINT ENABLER:
SPECTRUM

DISA CAMPAIGN PLAN JOINT ENABLER:
TESTING



The DISA Mission Partner Conference is co-sponsored by DISA and AFCEA.

The following are AFCEA events and programs only. These events are not co-sponsored by DISA or the Department of Defense.

DISA and the Department of Defense in no way endorse AFCEA, its events, programs, and sponsors. The appearance of any corporate advertisement or logo does not indicate any endorsement of that company or concern by DISA, the Department of Defense, or the federal government.

Attendance at and participation in any AFCEA event is purely voluntary.


www.DISA.mil